Generalized Factorial Functions and Binomial Coefficients

by

Andrew M. Crabbe

A departmental honors thesis submitted to the
Department of Mathematics at Trinity University
in partial fulfillment of the requirements for Graduation with departmental honors

April 20, 2001

Thesis Advisor

Department Chair

Interim Associate V.P. for Academic Affairs

ABSTRACT

Let $S \subseteq \mathbb{Z}$. The generalized factorial function for S, denoted $n!_S$, is introduced in accordance with theory already established by Bhargava ([4]). Along with several known theorems about these functions, a number of other issues will be explored. This Thesis is divided into 4 chapters. Chapter 1 provides the necessary definitions and offers a connection between the generalized factorial function and rings of integer-valued polynomials. In Chapter 2, necessary conditions on an infinite sequence of integers are obtained in order for that sequence to serve as the factorial sequence for some subset $S \subseteq \mathbb{Z}$. Chapter 3 explores the subject of !-equivalent subsets and we find a condition on two infinite subsets S and T of $\mathbb{Z}$ which force $n!_S = n!_T$ for every nonnegative integer n. We close in Chapter 4 with an analysis of generalized binomial coefficients, and for a given infinite subset $S \subseteq \mathbb{Z}$, we characterize those subsets $T \subseteq \mathbb{Z}$ for which $\binom{n}{m}_S = \binom{n}{m}_T$.

Contents

1 Introduction 1

2 Necessary Conditions on Factorial Sequences 7

3 !-Equivalent Subsets 14

4 Results Concerning Generalized Binomial Coefficients 19

A Appendix 24

1 Introduction

Most anyone who has taken an undergraduate course in abstract algebra should be somewhat familiar with the polynomial ring $\mathbb{Q}[x]$; that is, the the set containing all those polynomials, $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where the a_i's are in $\mathbb{Q}$. As such, $\mathbb{Q}[x]$ satisfies all the properties of a ring. In addition, $\mathbb{Q}[x]$ is closed under scalar multiplication from elements in $\mathbb{Q}$; so $\mathbb{Q}[x]$ is a vector space over the field $\mathbb{Q}$. For that reason, we can search for a basis of this vector space (i.e. a linearly independent subspace spanning $\mathbb{Q}[x]$). One's first choice, a correct one, might be $\{x^n\}_{n=0}^{\infty}$. However, for the purposes of this paper, there is a more interesting possibility, but first a definition.

Definition 1.1. Let n be a non-negative integer. If $n \geq 1$ then set

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

and if $n = 0$, $\binom{x}{0} = 1$.

This "more interesting" prospective basis is $\{\binom{x}{n}\}_{n=0}^{\infty}$, called the set of binomial polynomials. Let's consider a proof of this fact.

Proposition 1.2. *The set* $\{\binom{x}{n}\}_{n=0}^{\infty}$ *is a basis for the vector space* $\mathbb{Q}[x]$ *over* $\mathbb{Q}$.

Proof. There are two parts to this proof.

1) Show that $\{\binom{x}{n}\}_{n=0}^{\infty}$ spans $\mathbb{Q}[x]$ (i.e., every element of $\mathbb{Q}[x]$ can be expressed as a linear combination of elements in $\{\binom{x}{n}\}_{n=0}^{\infty}$). We use induction on the degree of the polynomial. For the initial case, let $f(x)$ be a polynomial in $\mathbb{Q}[x]$ of degree zero or, in other words, $f(x) = b_0$ where b_0 is in $\mathbb{Q}$. So $f(x) = b_0\binom{x}{0}$ and the initial case is proven. Now, assume that the property holds for all polynomials of degree $\leq n-1$. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial of degree n. Now $a_nn!\binom{x}{n}$ is a polynomial in $\mathbb{Q}[x]$ of degree n, whose x^n term has leading coefficient a_n. So, since the x^n terms will cancel, the rational polynomial $g(x) = f(x) - a_nn!\binom{x}{n}$ has degree $\leq n-1$, and from our assumption, $g(x) = \sum_{i=0}^{\infty} b_i\binom{x}{i}$. Thus $f(x) = a_nn!\binom{x}{n} + \sum_{i=0}^{\infty} b_i\binom{x}{i}$, which is the linear combination we're looking for. Thus, the property is proven for all rational polynomials.

2) Show that $\{\binom{x}{n}\}_{n=0}^{\infty}$ is a linearly independent set in $\mathbb{Q}[x]$. Let $f(x) = a_0 + a_1\binom{x}{1} + \cdots + a_n\binom{x}{n}$ be an arbitrary linear combination. Now, for $f(x) = 0$, it must be that the coefficient of the $\binom{x}{n}$ term is zero (i.e., $a_n = 0$) since it is the only $\binom{x}{i}$ which features such a term. For the same reason (coupled with the fact that $a_n = 0$), $a_{n-1} = 0$ and so on down the line, thus all coefficients are zero and the property is proven. □

We now turn to another ring, the set of all integer-valued polynomials (see [6]), denoted by Int($\mathbb{Z}$). This set is denoted by,

$$Int(\mathbb{Z}) = \{p(x) \in \mathbb{Q}[x] \mid p(z) \in \mathbb{Z}, \forall z \in \mathbb{Z}\}.$$

In other words, $\mathrm{Int}(\mathbb{Z})$ contains all those polynomials in $\mathbb{Q}[x]$ that map integers to integers. A few examples of polynomials in the set would be x, $3x^2 - 1$, or an integer such as 7. However $\mathrm{Int}(\mathbb{Z})$ contains more than just polynomials with integer-coefficients, such as those listed above. For instance, the polynomial $\frac{x(x-1)}{2}$ is in $\mathrm{Int}(\mathbb{Z})$ (since either z or $z-1$ is even for every z in $\mathbb{Z}$), as well as all the other binomial polynomials, as we show in the following lemma.

Lemma 1.3. *$\binom{x}{n} \in Int(\mathbb{Z})$, for all $n \geq 0$.*

Proof. Let n be arbitrary. If $\binom{x}{n} \in \mathrm{Int}(\mathbb{Z})$, then $\binom{a}{n} \in \mathbb{Z}$, for all $a \in \mathbb{Z}$. There are a number of cases to consider.

1) Let $a \geq n$. Then $\binom{a}{n}$ is a standard binomial coefficient, thus $\binom{a}{n} \in \mathbb{Z}$.

2) Let $0 \leq a \leq n-1$. By definition of $\binom{x}{n}$, $x - a$ is in the numerator, thus $\binom{a}{n} = 0$.

3) Let $a < 0$. Then,

$$\binom{a}{n} = \frac{a(a-1)\cdots(a-n+1)}{n!} =$$

$$(-1)^n \frac{(-a)(1-a)\cdots(n-1-a))}{n!} = (-1)^n \binom{n-1-a}{n}.$$

Thus the problem reduces to one of the two cases above. Therefore the proof is complete. □

Since $\mathrm{Int}(\mathbb{Z})$ is a ring, it is closed under addition and also closed under scalar multiplication with the integers. Although we can't properly consider $\mathrm{Int}(\mathbb{Z})$ to be a vector space (since $\mathbb{Z}$ is not a field), it is a $\mathbb{Z}$-module, which turns out to be enough for our purposes (see [7]). Much of the terminology remains the same, least of which is the concept of free basis (or $\mathbb{Z}$-basis, as it will be in this context), which carries over logically into the realm of modules. On that note, what are some possible $\mathbb{Z}$-bases for $\mathrm{Int}(\mathbb{Z})$? It would perhaps be appropriate to look at the example bases from $\mathbb{Q}[x]$. Upon immediate inspection, it can be seen that $\{x^n\}_{n=0}^{\infty}$ isn't satisfactory (for instance, there is no way to generate $\frac{x(x-1)}{2}$ from a linear combination of the elements in $\{x^n\}_{n=0}^{\infty}$ using only integer coefficients). But it so happens that the set, $\{\binom{x}{n}\}_{n=0}^{\infty}$, is in fact a $\mathbb{Z}$-basis.

Proposition 1.4. *The set $\{\binom{x}{n}\}_{n=0}^{\infty}$ is a $\mathbb{Z}$-basis for $Int(\mathbb{Z})$.*

Proof. Here we need to show independence over $\mathbb{Z}$ and spanning.

1) The independence of $\{\binom{x}{n}\}_{n=0}^{\infty}$ is shown similarly as in Proposition 1 above.

2) For spanning, it suffices to show that every polynomial in $\mathrm{Int}(\mathbb{Z})$ is a linear combination over $\mathbb{Z}$ of elements in $\{\binom{x}{n}\}_{n=0}^{\infty}$. To show this, we first need a couple of lemmas.

Lemma 1.5. *If $f(x)$ and $g(x)$ are polynomials of degree $\leq n$ in $\mathbb{Q}[x]$ and $f(0) = g(0)$, $f(1) = g(1)$, ..., $f(n) = g(n)$, then $f(x) = g(x)$.*

Proof. Using the premises, the polynomial $f(x) - g(x)$ has degree $\leq n$; thus the equation $f(x) - g(x) = 0$ has at most n distinct roots (if it is not equivalently the zero-polynomial). However it has been assumed that $f(x) = g(x)$ at least $n+1$ values; thus $f(x) - g(x) = 0, \forall x$, and $f(x) = g(x)$. □

Lemma 1.6. *Given a sequence of integers, $b_0, b_1, \dots, b_n$, there is a polynomial $g(x) = c_0\binom{x}{0} + c_1\binom{x}{1} + \cdots + c_n\binom{x}{n}, c_i \in \mathbb{Z}, \forall i$ such that $g(0) = b_0, g(1) = b_1, \dots, g(n) = b_n$.*

Proof. The proof will be by induction on the length of the integer sequence.

1) Let the sequence, b_0, be of length one. Then $g(x) = b_0\binom{x}{0}$.

2) Assume that the property holds for sequences of length $\leq n$. Given the sequence $b_0, b_1, \dots, b_n$, we find a corresponding $g(x)$. From the assumption, there exists a $f(x) = \sum_{i=0}^{n-1} c_i\binom{x}{i}$ for which

$$f(0) = b_0, f(1) = b_1, \dots, f(n-1) = b_{n-1}.$$

Consider the polynomial $g(x) = f(x) + (b_n - f(n))\binom{x}{n}$. Now, for all i such that $0 \leq i \leq n-1$, $\binom{i}{n} = 0$ (for $(x-i)$ is in the numerator of $\binom{x}{n}$). Thus $g(i) = f(i) = b_i, \forall 0 \leq i \leq n-1$. Now, at n, $g(n) = f(n) + (b_n - f(n))\binom{n}{n} = f(n) + b_n - f(n) = b_n$. So with $g(x) = f(x) + (b_n - f(n))\binom{x}{n}$, an appropriate polynomial has been found, and the lemma has been proved. □

We return to the proof of Proposition 4. Let $f(x)$ be a polynomial in $\mathrm{Int}(\mathbb{Z})$ with degree n, and let $f(0) = b_0, f(1) = b_1, \dots, f(n) = b_n$. By Lemma 1.6, there is a polynomial $g(x) = \sum_{i=0}^{n-1} c_1\binom{x}{i}$ for which $g(0) = f(0)$, $g(1) = f(1)$, $\dots$, $g(n) = f(n)$. By Lemma 1.5, $f(x) = g(x), \forall x$. Thus the proof is complete. □

We now introduce a new ring. If S is a subset of $\mathbb{Z}$, set

$$Int(S, \mathbb{Z}) = \{p(x) \in \mathbb{Q}[x] \mid p(s) \in \mathbb{Z}, \forall s \in S\}.$$

In other words, $\mathrm{Int}(S, \mathbb{Z})$ contains all those polynomials in $\mathbb{Q}[x]$ that are integer-valued at the elements of S. An easy observation about this ring is that $\mathrm{Int}(\mathbb{Z}) \subseteq \mathrm{Int}(S, \mathbb{Z})$ (since a polynomial that is integer-valued for all integers must be integer-valued for any subset, S, of the integers). Again, for reasons similar to the above, $\mathrm{Int}(S, \mathbb{Z})$ is a $\mathbb{Z}$-module. What else can we say about $\mathrm{Int}(S, \mathbb{Z})$? More specifically, can we determine any $\mathbb{Z}$-bases? In order to approach these questions more intelligently, with some hope of success, we turn to Bhargava and his work on generalizing the factorial function for subsets of $\mathbb{Z}$ (see [3] and [4]).

At the foundation of Bhargava's theory is a notion called a p-ordering of S (where S is an arbitrary subset of $\mathbb{Z}$). A p-ordering of S is a sequence, $\{a_i\}_{i=0}^{\infty}$, of elements in S constructed in the following manner.

Select any element in S, and denote it as a_0.

Select an element $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$.

Select an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$.

In general, select an element $a_k \in S$ that minimizes the highest power of p dividing $(a_k - a_0)(a_k - a_1) \cdots (a_k - a_{k-1})$.

It should be immediately apparent that there is no unique p-ordering of S since, among other reasons, a_0 is chosen arbitrarily (there could also be any number of elements minimizing the product at any particular point, from which you can only pick one). Now, if we are given a particular p-ordering of S, we can define a new sequence, $\{\nu_k(S,p)\}_{i=0}^{\infty}$, called the associated p-sequence of S. For each $k \geq 0$, let $\nu_k(S,p)$ be the power of p minimized at the kth step in the p-ordering process. In other words,

$$\nu_k(S,p) = w_p((a_k - a_0) \cdots (a_k - a_{k-1}))$$

where $w_p(a)$ represents the highest power of p dividing a (for instance, $w_5(50) = 25$). From the construction of the p-ordering, it is easy to see that such a sequence must be monotone increasing. What is truly amazing about these associated p-sequences is that they are entirely independent of the choice of p-ordering!

Theorem 1.7. *[4, Theorem 5] The associated p-sequence, $\{\nu_k(S,p)\}_{k=0}^{\infty}$, is independent of the particular choice of p-ordering of S.*

To better understand the construction of a p-ordering, we consider $\mathbb{Z}$ itself.

Proposition 1.8. *[4, Proposition 6] The ordering $0, 1, 2, \ldots$ forms a natural p-ordering of $\mathbb{Z}$ for all primes p.*

Proof. We again use induction.

1) The a_0 can be chosen arbitrarily, so choose 0. By selecting $a_1 = 1$, $a_1 - a_0 = 1 - 0 = 1$ which obviously minimizes the power of p dividing $a_1 - a_0$ for all primes p.

2) Assume that the property holds for the first $k-1$ steps (i.e., the ordering thus far is $0, 1, 2, \ldots, k-1$). In the kth step, we want to minimize the power of p dividing $(a_k - 0)(a_k - 1) \cdots (a_k - (k-1))$. But regardless of our choice of a_k, the product is a product of k consecutive integers, thus divisible by $k!$. But this $k!$ can be had if k is selected as the a_k, which would clearly minimize the power of p dividing the product for all primes. Thus the proof is complete. □

With this natural p-ordering, we can determine the unique associated p-sequence for $\mathbb{Z}$ as follows:

$$\nu_k(\mathbb{Z},p) = w_p((a_k - a_0) \cdots (a_k - a_{k-1})) = w_p((k-0) \cdots (k-(k-1))) = w_p(k!).$$

Notice that if we were to fix k and have p range over all primes, taking the product of all the resulting $\nu_k(\mathbb{Z},p)$'s would yield the prime factorization of $k!$. Thus we can represent $k!$ purely as a product of these $\nu_k(\mathbb{Z},p)$'s (which are invariant in $\mathbb{Z}$) as,

$$k! = \prod_p \nu_k(\mathbb{Z},p).$$

But since each subset, S, has its own invariant $\nu_k(S,p)$'s, we can similarly define the generalized factorial function, $k!_S$, as follows:

$$k!_S = \prod_p \nu_k(S,p).$$

If, as in the case with $\mathbb{Z}$, there is a p-ordering, $\{a_i\}_{i=0}^{\infty}$,which holds for all primes simultaneously, then $k!_S$ can be written more simply as $k!_S = \mid (a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1}) \mid$ (see [4, Lemma 16]).

Let's look at a few examples of the generalized factorial function in various subsets of $\mathbb{Z}$. (These examples are taken from [4].)

Example 1.9. Let $S = 2\mathbb{Z}$ (i.e. S is the set of even integers). Like $\mathbb{Z}$ before, there is a natural p-ordering $0, 2, 4, \ldots$ which holds for all primes p. Thus

$$k!_{2\mathbb{Z}} = (2k-0)(2k-2)\cdots(2k-(2k-2)) = 2^k k!.$$

Example 1.10. Let S be the set of powers of 2 (which are in $\mathbb{Z}$). Again there is a natural ordering $1, 2, 4, 8, \ldots$ holding for all primes p. Here

$$k!_S = (2^k - 1)(2^k - 2)\cdots(2^k - 2^{k-1}).$$

Example 1.11. Let S be the set of all squares in $\mathbb{Z}$, which we denote by $\mathbb{Z}^S$. There is a natural ordering $0, 1, 4, 9, \ldots$ which holds for all primes. So

$$k!_{\mathbb{Z}^S} = (k^2 - 0)(k^2 - 1)\cdots(k^2 - (k-1)^2)) = \frac{(2k)!}{2}.$$

The task of calculating the generalized factorial function for subsets such as these (subsets that are well-structured and bear a natural p-ordering that holds for all primes) is relatively straightforward; though this is certainly not the case with more "perverse" subsets. For instance, when S is the set of all primes, we get the result (from [4]):

$$k!_S = \prod_p p^{\lfloor \frac{k-1}{p-1} \rfloor + \lfloor \frac{k-1}{p(p-1)} \rfloor + \lfloor \frac{k-1}{p^2(p-1)} \rfloor + \cdots}.$$

Moving on, since $k!_S$ is called a generalized factorial function, we would expect it to share some of the properties held by the traditional factorial function, $k!$. A familiar property of the factorial is that for any nonnegative integers n and m, $n!m! \mid (n+m)!$. A proof of this fact could be presented rather easily, though it's sufficient for our purposes just to recall that the binomial coefficient, $\binom{n+m}{n} = \frac{(n+m)!}{n!m!}$, is integer-valued. It is hoped that the same could be said in the general case (i.e., for any nonnegative integers n and m, $n!_S m!_S \mid (n+m)!_S$). This property is proven in Bhargava (see [4, Theorem 8]), though not without difficulty (and a number of lemmas), so let the truth of the statement stand without explicit substantiation. Now with this being true, we can define something called the generalized binomial coefficient for S in the logical way:

$$\binom{n}{k}_S = \frac{n!_S}{k!_S(n-k)!_S}.$$

These coefficients become quite interesting. Each subset of $\mathbb{Z}$ has a characteristic set of binomial coefficients, so each will have its own Pascal's Triangle and no doubt a whole range of other interesting characteristics. Returning to Examples 1.9 and 1.11 above, it can be shown, by easy calculation, that $\binom{n}{k}_{2\mathbb{Z}} = \binom{n}{k}$, and $\binom{n}{k}_{\mathbb{Z}^S} = 2\binom{2n}{2k}$.

It would perhaps be an appropriate time to recall the reason why we found the need to define these p-orderings, generalized factorials, etc. It was our intent to find a basis for the $\mathbb{Z}$-module, $\mathrm{Int}(S, \mathbb{Z})$. Recall that for $\mathrm{Int}(\mathbb{Z})$ (which could also be written $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$), the basis that we presented was the set of binomial polynomials, $\{\binom{x}{n}\}_{n=0}^{\infty}$, where

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-k+1)}{n!}.$$

Given our new knowledge of p-orderings (specifically that the sequence $0, 1, 2, \ldots$ forms a p-ordering, $\{a_i\}_{i=0}^{\infty}$, on $\mathbb{Z}$ for all primes p), we can re-express this polynomial as

$$\binom{x}{n} = \frac{(x-a_0)(x-a_1)\cdots(x-a_{k-1})}{n!_{\mathbb{Z}}}.$$

We can extend these conclusions further, but first a definition.

Definition 1.12. Let $\{a_{i,k}\}_{i=0}^{\infty}$ be a sequence in $\mathbb{Z}$ that, for each prime p dividing $k!_S$, is termwise congruent modulo $\nu_k(S, p)$ to some p-ordering of S.

The purpose of defining such a sequence is that, usually, there is no particular ordering of elements in S that satisfies the p-ordering requirements for all primes p less than some fixed integer (let alone all primes). This sequence at least gives an ordering respecting the idiosyncrasies that exist between p-orderings of primes under a certain bound. But now we state the theorem.

Theorem 1.13. *The set $\{\binom{x}{n}_S\}_{n=0}^{\infty}$ forms a basis for the $\mathbb{Z}$-module Int$(S, \mathbb{Z})$, where*

$$\binom{x}{n}_S = \frac{(x-a_{0,n})(x-a_{1,n})\cdots(x-a_{n-1,n})}{n!_S}.$$

As I don't intend to offer a proof of this theorem, the interested reader can see [4] for more details (see [4, Theorem 23]). For our purposes, the most important feature of this theorem is that it presents an instance, a context, in which the generalized factorial function reveals itself. (And it, of course, has historical significance, as these leading coefficients were the inspiration for Bhargava's theory).

The purpose of this paper is to further the theory already established by Bhargava. Three general areas of interest will be examined: (i) what are necessary conditions on a factorial sequence, (ii) criteria for !-equivalence of subsets in $\mathbb{Z}$, and (iii) the theory of generalized binomial coefficients.

2 Necessary Conditions on Factorial Sequences

Before proceeding further, it would be best to mention a case which isn't mentioned explicitly in Bhargava, that in which $S \subseteq \mathbb{Z}$ is a finite subset. This undoubtedly yields different results. For instance, if $|S| = n$, then the construction of the p-ordering must begin repeating elements after the $(n-1)$st step (so the product, $(a_k - a_0)(a_k - a_1) \cdots (a_k - a_{k-1}) = 0$, for $k \geq n$). As a result, the definition of the generalized factorial function,

$$k!_S = \prod_p \nu_k(S,p) = \prod_p w_p((a_k - a_0) \cdots (a_k - a_{k-1})),$$

seems to lose meaning for $k \geq n$. I think it would make the most sense to regard $k!_S$ as equalling 0 for $k \geq n$ (as this stipulation would preserve $n!_S m!_S \mid (n+m)!_S$). But this does little to illuminate the structure of $\text{Int}(S, \mathbb{Z})$, since $\binom{x}{k}_S$ is undefined for $k \geq n$. Because of its somewhat "diseased" nature, the finite case will be occasionally ignored (though not without warning). Thankfully however, the generation of the factorial sequence for finite subsets lends itself well to programming (see Appendix for such a MAPLE creation).

The following theorem describes an extremely important property of generalized factorial functions. Its usefulness cannot be understated.

Theorem 2.1. *[4, Lemma 13] Let $S \subseteq T$. Then $n!_T | n!_S$, $\forall n \geq 0$.*

Proof. Though Bhargava proves this in his paper, there is a rather clever proof involving what we know about integer-valued polynomial rings which is perhaps a bit more direct. Since $S \subseteq T$, $\text{Int}(T, \mathbb{Z}) \subseteq \text{Int}(S, \mathbb{Z})$ (since a polynomial that is integer-valued for all integers in T must be integer-valued for any subset, S, of T). Now $\{\binom{x}{i}_S\}_{i=0}^{\infty}$ is a $\mathbb{Z}$-basis for $\text{Int}(S, \mathbb{Z})$. The most pertinent characteristic of $\binom{x}{i}_S$ is that its leading coefficient is $\frac{1}{i!_S}$. Since $\text{Int}(T, \mathbb{Z}) \subseteq \text{Int}(S, \mathbb{Z})$, $\binom{x}{n}_T$ can be expressed as a linear combination of $\binom{x}{i}_S$'s with integer coefficients (where $0 \leq i \leq n$). So,

$$\binom{x}{n}_T = z_n \binom{x}{n}_S + z_{n-1} \binom{x}{n-1}_S + \cdots + z_1 \binom{x}{1} + z_0 \binom{x}{0}_S.$$

¿From the fact that the leading coefficient of $\binom{x}{n}_T$ (a polynomial of degree n) is $\frac{1}{n!_T}$ and that the leading coefficient of the degree-n term on the right side is $\frac{z_n}{n!_S}$(from $z_n \binom{x}{n}_S$), it must be that $\frac{1}{n!_T} = \frac{z_n}{n!_S}$. Or in other words, $z_n n!_T = n!_S$. Therefore $n!_T | n!_S = \alpha_n$, for all $n \geq 0$. □

This makes intuitive sense since if we have more elements from which to choose (as we would with T), the likelihood of finding a more minimizing element in a p-ordering is increased.

We can readily recognize $1, 1, 2, 6, 24, 120, 720, \ldots$ as the factorial sequence for $\mathbb{Z}$; and with a bit more familiarity with generalized factorial functions, we can recognize 1, 2, 8, 48, 384,... as the factorial sequence for $2\mathbb{Z}$. But for an arbitrary infinite integer sequence,

$\alpha_0, \alpha_1, \alpha_2, \ldots$, how do we know whether there exists an $S \subseteq \mathbb{Z}$ such that the above is its factorial sequence? To this effect, the following is a list of conditions on $\alpha_0, \alpha_1, \alpha_2, \ldots$ which are necessary for the existence of such an S.

Theorem 2.2. *Let $\alpha_0, \alpha_1, \alpha_2, \ldots$ be an infinite sequence of integers. If there exists an $S \subseteq \mathbb{Z}$ such that the above is its factorial sequence (i.e., $n!_S = \alpha_n$), then the following are necessary:*

i) $\alpha_i \alpha_j \mid \alpha_{i+j}$, for $i, j \geq 0$.

ii) $\alpha_0 = 0!_S = 1$

iii) $n! \mid n!_S = \alpha_n$, for all $n \geq 0$.

iv) Let $\alpha_1 = 1!_S = l$. Then $l^n n! \mid \alpha_n$, for all $n \geq 0$. (And this is the strongest claim we can make, given only the value for α_1.)

v) Let $\alpha_1 = 1!_S = l = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u}$ and $\alpha_2 = 2!_S = l^2 m_2 2!$, where $m_2 2! = r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_v^{\gamma_v}$ (with $p, r \in \mathbb{P}$). Then considering all $q \in \mathbb{P}$, where $w_q(l) = q^\beta$ and $w_q(m_2 2!) = q^\gamma$,

$$\prod_{\substack{q \mid m_2 \\ q \nmid l}} q^{\gamma \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2q} \rfloor + \lfloor \frac{n}{2q^2} \rfloor + \cdots} \prod_{\substack{q \mid m_2 \\ q \mid l}} q^{(2\beta+\gamma) \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2q} \rfloor + \lfloor \frac{n}{2q^2} \rfloor + \cdots}$$

$$\prod_{\substack{q \nmid m_2 \\ q \mid l}} q^{n\beta} \cdot \nu_n(\mathbb{Z}, q) \prod_{\substack{q \nmid m_2 \\ q \nmid l}} \nu_n(\mathbb{Z}, q) \ \ \mid \ n!_S = \alpha_n \ .$$

Proof. i) This is a result of Bhargava (see [4, Theorem 8]).

ii) We have defined $0!_S$ to be 1 for all $S \subseteq \mathbb{Z}$, so no proof is needed.

iii) This is a special case of Theorem 2.1 above. Here we just allow that $T = \mathbb{Z}$.

iv) Let $\alpha_1 = 1!_S = l$. Now if $l = 1$, then we need to prove that $1^n n! = n! \mid n!_S$. But this is merely a restatement of (iii), so we are done. So let $l = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u}$, where the p_i's are distinct primes with $\beta_i \geq 1$. Choose an arbitrary prime divisor, p_i, of l (where $p_i^{\beta_i} \mid l$ but $p_i^{\beta_i+1} \nmid l$). Let $a_0, a_1, a_2, \ldots$ be a p_i-ordering for S. Since $\nu_1(S, p_i) = p_i^{\beta_i}$, $\ p_i^{\beta_i} \mid (a - a_0)$ for all $a \in S$. In other words, $\forall a \in S$, $a \equiv a_0 \equiv b_i (\text{mod } p_i^{\beta_i})$ where $0 \leq b_i < p_i^{\beta_i}$ is fixed. So generally, $\forall a \in S$

$$a \equiv b_1 (\text{mod } p_1^{\beta_1})$$

$$a \equiv b_2 (\text{mod } p_2^{\beta_2})$$

$$\vdots$$

$$a \equiv b_u (\text{mod } p_u^{\beta_u}).$$

So by the Chinese Remainder Theorem, there exists a b such that

$$a \equiv b (\bmod\ p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u}),$$

or

$$a \equiv b (\bmod\ l).$$

The largest set in which this holds is obviously $T = l\mathbb{Z} + b$, so $S \subseteq T$. From [4, Example 17], we have that $n!_T = l^n n!$. Therefore by Theorem 2.1, $l^n n! \mid n!_S = \alpha_n$, for all $n \geq 0$.

(v) Let $1!_S = l = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u}$ and $2!_S = l^2 m_2 2!$, where $m_2 2! = r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_v^{\gamma_v}$ (with $p, r \in \mathbb{P}$). There are four types of primes, q, to consider.

a) Consider those q such that $q \mid m_2$ but $q \nmid l$. Let q be an arbitrary prime of this type, where $\nu_2(S, q) = q^\gamma$. So for a q-ordering of S, beginning $a_0, a_1, a_2, \ldots$, we have that $w_q((a_2 - a_1)(a_2 - a_0)) = q^\gamma$. It must be that $w_q(a_2 - a_1) = q^\gamma$ and $w_q(a_2 - a_0) = 1$ or vice versa, since if $q \mid (a_2 - a_1)$ and $q \mid (a_2 - a_0)$, then $q \mid (a_1 - a_0)$. In this case, $q \mid l$, which violates our assumption about q. So if $a_1 \equiv c (\bmod\ q^\gamma)$ and $a_0 \equiv d (\bmod\ q^\gamma)$, we have that, $\forall s \in S$, $s \equiv c$ or $d (\bmod\ q^\gamma)$. The largest subset, T, such that $\forall t \in T$, $t \equiv c$ or $d (\bmod\ q^\gamma)$ is $T = (q^\gamma \mathbb{Z} + c) \cup (q^\gamma \mathbb{Z} + d)$.

Now we construct the q-ordering for T.

Claim: $c, d, q^\gamma + c, q^\gamma + d, 2q^\gamma + c, 2q^\gamma + d, \ldots$ is a q-ordering for T. Generally, if n is even, $a_n = \frac{n}{2} q^\gamma + c$, and if n is odd, $a_n = \frac{n-1}{2} q^\gamma + d$.

Since verifying this claim is rather tedious, the proof of it is left to the Appendix (Notes A.1).

With the q-ordering constructed, we can solve for $\nu_n(T, q)$. We need to consider separately the cases in which n is even and when n is odd.

If n is even,

$$\nu_n(T,q) = w_q((\frac{n}{2}q^\gamma + c - \frac{n-2}{2}q^\gamma - d)(\frac{n}{2}q^\gamma + c - \frac{n-2}{2}q^\gamma - c) \cdots \\ (\frac{n}{2}q^\gamma + c - d)(\frac{n}{2}q^\gamma + c - c)).$$

And since $w_q(kq^\gamma + (c - d)) = 1$, $\forall k \in \mathbb{Z}$,

$$= w_q((\frac{n}{2} - \frac{n-2}{2})q^\gamma \cdots (\frac{n}{2} - 1)q^\gamma (\frac{n}{2})q^\gamma) = q^{\frac{n\gamma}{2}} w_q(\frac{n}{2}!)$$

$$= q^{\gamma \lfloor \frac{n}{2} \rfloor} \cdot q^{\lfloor \frac{n}{2q} \rfloor + \lfloor \frac{n}{2q^2} \rfloor + \lfloor \frac{n}{2q^3} \rfloor + \cdots} = q^{\gamma \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2q} \rfloor + \lfloor \frac{n}{2q^2} \rfloor + \lfloor \frac{n}{2q^3} \rfloor + \cdots}.$$

(For explanation of why $w_q(\frac{n}{2}!) = q^{\lfloor \frac{n}{2q} \rfloor + \lfloor \frac{n}{2q^2} \rfloor + \lfloor \frac{n}{2q^3} \rfloor + \cdots}$, see Notes A.2 in Appendix.)

If n is odd,

$$\nu_n(T,q) = w_q((\frac{n-1}{2}q^\gamma + d - \frac{n-1}{2}q^\gamma - c)(\frac{n-1}{2}q^\gamma + d - \frac{n-3}{2}q^\gamma - d)\cdots$$
$$(\frac{n-1}{2}q^\gamma + d - d)(\frac{n-1}{2}q^\gamma + d - c))$$

$$= w_q((\frac{n-1}{2} - \frac{n-3}{2})q^\gamma \cdots (\frac{n-1}{2} - 1)q^\gamma(\frac{n-1}{2})q^\gamma) = q^{\frac{(n-1)\gamma}{2}} w_q(\frac{n-1}{2}!)$$

$$= q^{\gamma\lfloor\frac{n-1}{2}\rfloor} \cdot q^{\lfloor\frac{n-1}{2q}\rfloor + \lfloor\frac{n-1}{2q^2}\rfloor + \lfloor\frac{n-1}{2q^3}\rfloor + \cdots} = q^{\gamma\lfloor\frac{n}{2}\rfloor} \cdot q^{\lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots}$$

$$= q^{\gamma\lfloor\frac{n}{2}\rfloor + \lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots}.$$

(For explanation of why $\lfloor\frac{n}{2q^r}\rfloor = \lfloor\frac{n-1}{2q^r}\rfloor$, see Notes A.3 in Appendix.)

Thus $\forall n \geq 0$, we have that

$$\nu_n(T,q) = q^{\gamma\lfloor\frac{n}{2}\rfloor + \lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots}.$$

And since $S \subseteq T$, $\nu_n(T,q) \mid \nu_n(S,q)$ or

$$q^{\gamma\lfloor\frac{n}{2}\rfloor + \lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots} \mid \nu_n(S,q).$$

b) Consider those q such that $q \mid m_2$ and $q \mid l$. Let q be an arbitrary prime of this type, where $\nu_1(S,q) = q^\beta$ and $\nu_2(S,q) = q^{2\beta} \cdot q^\gamma$. So for a q-ordering of S beginning $a_0, a_1, a_2, \ldots$, we have that $w_q(a_1 - a_0) = q^\beta$ and $w_q((a_2 - a_1)(a_2 - a_0)) = q^{2\beta} \cdot q^\gamma$. It must be that $w_q(a_2 - a_1) = q^{\beta+\gamma}$ and $w_q(a_2 - a_0) = q^\beta$ or vice versa. This is because $q^\beta \mid (a_2 - a_1)$ and $q^\beta \mid (a_2 - a_0)$ (else $\nu_1(S,q) < q^\beta$, which is a contradiction); and if $q^{\beta+1} \mid (a_2 - a_1)$ and $q^{\beta+1} \mid (a_2 - a_0)$, then $a_1 \equiv a_0 (\text{mod } q^{\beta+1})$ (which implies that $q_{\beta+1} \mid w_q(a_1 - a_0) = q^\beta$, another contradiction). So if $a_1 \equiv c (\text{mod } q^{\beta+\gamma})$ and $a_0 \equiv d (\text{mod } q^{\beta+\gamma})$ (where $w_q(c-d) = q^\beta$), we have that, $\forall s \in S$, $s \equiv c$ or $d (\text{mod } q^{\beta+\gamma})$. The largest subset, T, such that $\forall t \in T$, $t \equiv c$ or $d (\text{mod } q^{\beta+\gamma})$ is $T = (q^{\beta+\gamma}\mathbb{Z} + c) \cup (q^{\beta+\gamma}\mathbb{Z} + d)$.

Similar to the above case, $c, d, q^{\beta+\gamma} + c, q^{\beta+\gamma} + d, 2q^{\beta+\gamma} + c, 2q^{\beta+\gamma} + d, \ldots$ is a q-ordering for T. This can be shown in a proof analogous to that for the above, so we leave the details to the reader. In order to determine $\nu_n(T,q)$, we must again consider the parity of n.

If n is even,

$$\nu_n(T,q) = w_q((\frac{n}{2}q^{\beta+\gamma} + c - \frac{n-2}{2}q^{\beta+\gamma} - d)(\frac{n}{2}q^{\beta+\gamma} + c - \frac{n-2}{2}q^{\beta+\gamma} - c)\cdots$$
$$(\frac{n}{2}q^{\beta+\gamma} + c - d)(\frac{n}{2}q^{\beta+\gamma} + c - c))$$

$$\begin{aligned}&= w_q((\frac{n}{2}q^{\beta+\gamma} - \frac{n-2}{2}q^{\beta+\gamma})(\frac{n}{2}q^{\beta+\gamma} - \frac{n-4}{2}q^{\beta+\gamma}) \cdots (\frac{n}{2}q^{\beta+\gamma} - q^{\beta+\gamma})(\frac{n}{2}q^{\beta+\gamma})) \cdot \\ &\quad w_q((\frac{n}{2}q^{\beta+\gamma} - \frac{n-2}{2}q^{\beta+\gamma} + (c-d))(\frac{n}{2}q^{\beta+\gamma} - \frac{n-4}{2}q^{\beta+\gamma} + (c-d)) \cdots \\ &\qquad (\frac{n}{2}q^{\beta+\gamma} - q^{\beta+\gamma} + (c-d))(\frac{n}{2}q^{\beta+\gamma} + (c-d))).\end{aligned}$$

And since, $w_q(kq^{\beta+\gamma} + (c-d)) = q^{\beta}$,

$$= w_q((\frac{n}{2} - \frac{n-2}{2})q^{\beta+\gamma} \cdots (\frac{n}{2} - 1)q^{\beta+\gamma}(\frac{n}{2})q^{\beta+\gamma}) \cdot q^{\beta\frac{n}{2}} = q^{\frac{n(\beta+\gamma)}{2}} w_q(\frac{n}{2}!) \cdot q^{\frac{n\beta}{2}}$$

$$= q^{\frac{n(2\beta+\gamma)}{2}} w_q(\frac{n}{2}!) = q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor} \cdot q^{\lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots}$$

$$= q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor + \lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots}.$$

If n is odd,

$$\begin{aligned}\nu_n(T, q) &= w_q((\frac{n-1}{2}q^{\beta+\gamma} + d - \frac{n-1}{2}q^{\beta+\gamma} - c)(\frac{n-1}{2}q^{\beta+\gamma} + d - \frac{n-3}{2}q^{\beta+\gamma} - d) \cdots \\ &\qquad (\frac{n-1}{2}q^{\beta+\gamma} + d - d)(\frac{n-1}{2}q^{\beta+\gamma} + d - c))\end{aligned}$$

$$\begin{aligned}&= w_q((\frac{n-1}{2}q^{\beta+\gamma} - \frac{n-3}{2}q^{\beta+\gamma})(\frac{n-1}{2}q^{\beta+\gamma} - \frac{n-5}{2}q^{\beta+\gamma}) \cdots \\ &\qquad (\frac{n-1}{2}q^{\beta+\gamma} - q^{\beta+\gamma})(\frac{n-1}{2}q^{\beta+\gamma})) \cdot \\ &\quad w_q((\frac{n-1}{2}q^{\beta+\gamma} - \frac{n-1}{2}q^{\beta+\gamma} + (d-c))(\frac{n-1}{2}q^{\beta+\gamma} - \frac{n-3}{2}q^{\beta+\gamma} + (d-c)) \cdots \\ &\qquad (\frac{n-1}{2}q^{\beta+\gamma} - q^{\beta+\gamma} + (d-c))(\frac{n-1}{2}q^{\beta+\gamma} + (d-c))).\end{aligned}$$

$$= w_q((\frac{n-1}{2} - \frac{n-3}{2})q^{\beta+\gamma} \cdots (\frac{n-1}{2} - 1)q^{\beta+\gamma}(\frac{n-1}{2})q^{\beta+\gamma}) \cdot q^{\beta\frac{n-1}{2}}$$

$$= q^{\frac{(n-1)(\beta+\gamma)}{2}} w_q(\frac{n-1}{2}!) \cdot q^{\frac{(n-1)\beta}{2}} = q^{\frac{(n-)(2\beta+\gamma)}{2}} w_q(\frac{n-1}{2}!)$$

$$= q^{(2\beta+\gamma)\lfloor\frac{n-1}{2}\rfloor} \cdot q^{\lfloor\frac{n-1}{2q}\rfloor + \lfloor\frac{n-1}{2q^2}\rfloor + \lfloor\frac{n-1}{2q^3}\rfloor + \cdots} = q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor} \cdot q^{\lfloor\frac{n}{2q}\rfloor + \lfloor\frac{n}{2q^2}\rfloor + \lfloor\frac{n}{2q^3}\rfloor + \cdots}$$

$$= q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{2q}\rfloor+\lfloor\frac{n}{2q^2}\rfloor+\lfloor\frac{n}{2q^3}\rfloor+\cdots}.$$

Thus $\forall n \geq 0$, we have that

$$\nu_n(T,q) = q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{2q}\rfloor+\lfloor\frac{n}{2q^2}\rfloor+\lfloor\frac{n}{2q^3}\rfloor+\cdots}.$$

And since $S \subseteq T$, $\nu_n(T,q) \mid \nu_n(S,q)$ or

$$q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{2q}\rfloor+\lfloor\frac{n}{2q^2}\rfloor+\lfloor\frac{n}{2q^3}\rfloor+\cdots} \mid \nu_n(S,q).$$

c) Consider those q such that $q \nmid m_2$ and $q \mid l$. So let $q \neq 2$ be a prime of this type, where $\nu_1(S,q) = q^\beta$ and $\nu_2(S,q) = q^{2\beta}$ ($q = 2$ is a special case which will be treated later). So, for a q-ordering of S beginning $a_0, a_1, a_2, \ldots$, we have that $w_q(a_1 - a_0) = q^\beta$ and $w_q((a_2 - a_1)(a_2 - a_0)) = q^{2\beta}$. It must be that $w_q(a_2 - a_1) = q^\beta$ and $w_q(a_2 - a_0) = q^\beta$, since $q^\beta \mid (a_2 - a_1)$ and $q^\beta \mid (a_2 - a_0)$ (else $\nu_1(S,q) < q^\beta$, which is a contradiction). So the strongest statement we can make is that $\forall a \in S$, $a \equiv a_0 \equiv a_1 \equiv b (\text{mod } q^\beta)$. The largest subset, T, such that $\forall t \in T$, $t \equiv a_0 \equiv a_1 \equiv b (\text{mod } q^\beta)$ is $T = q^\beta\mathbb{Z} + b$. Since $S \subseteq T$, we have that $\forall n \geq 0$,

$$\nu_n(T,q) = q^{n\beta} \cdot \nu_n(\mathbb{Z},q) \mid \nu_n(S,q).$$

Now let $q = 2$, where $\nu_1(S,2) = 2^\beta$ and $\nu_2(S,2) = 2^{2\beta} \cdot 2 = 2^{2\beta+1}$. So for a 2-ordering of S, beginning $a_0, a_1, a_2, \ldots$, it must be that $w_2(a_2 - a_1) = 2^{\beta+1}$ and $w_q(a_2 - a_0) = 2^\beta$ or vice versa. This is because $2^\beta \mid (a_2 - a_1)$ and $2^\beta \mid (a_2 - a_0)$ (else $\nu_1(S,2) < 2^\beta$, which is a contradiction). So, if $a_1 \equiv c(\text{mod } 2^{\beta+1})$ and $a_0 \equiv d(\text{mod } 2^{\beta+1})$ (where $w_q(c - d) = q^\beta$), we have that $\forall s \in S$, $s \equiv c$ or $d(\text{mod } 2^{\beta+1})$. The largest subset, T, such that $\forall t \in T$, $t \equiv c$ or $d(\text{mod } 2^{\beta+1})$ is $T = (2^{\beta+1}\mathbb{Z} + c) \cup (2^{\beta+1}\mathbb{Z} + d)$. Consider the set $2^\beta\mathbb{Z} + c$.

Claim: $2^\beta\mathbb{Z} + c = (2^{\beta+1}\mathbb{Z} + c) \cup (2^{\beta+1}\mathbb{Z} + d) = T$.

Now, let $t \in 2^\beta\mathbb{Z} + c$. So $t \equiv c(\text{mod } 2^\beta)$ and either $t \equiv c(\text{mod } 2^{\beta+1})$ or $t \equiv c + 2^\beta(\text{mod } 2^{\beta+1})$. Since $d \equiv c(\text{mod } 2^\beta)$ and $d \not\equiv c(\text{mod } 2^{\beta+1})$, $d \equiv c + 2^\beta(\text{mod } 2^{\beta+1})$. So either $t \equiv c(\text{mod } 2^{\beta+1})$ or $t \equiv d(\text{mod } 2^{\beta+1})$. Thus $t \in (2^{\beta+1}\mathbb{Z} + c) \cup (2^{\beta+1}\mathbb{Z} + d)$. Therefore $2^\beta\mathbb{Z} + c \subseteq T$.

Now, let $t \in (2^{\beta+1}\mathbb{Z} + c) \cup (2^{\beta+1}\mathbb{Z} + d)$. So $t \equiv c(\text{mod } 2^{\beta+1})$ or $t \equiv d(\text{mod } 2^{\beta+1})$. Since $c \equiv d(\text{mod } 2^\beta)$, $t \equiv c(\text{mod } 2^\beta)$, leaving $t \in 2^\beta\mathbb{Z} + c$. Thus $T \subseteq 2^\beta\mathbb{Z} + c$.

This proves $T = 2^\beta\mathbb{Z} + c$. So since $S \subseteq T$,

$$\nu_n(T,2) = 2^{n\beta} \cdot \nu_n(\mathbb{Z},2) \mid \nu_n(S,2),$$

which is in the same form as the above. Therefore $\forall n \geq 0$, and all q such that $q \nmid m_2$ and $q \mid l$, we have that

$$q^{n\beta} \cdot \nu_n(\mathbb{Z},q) \mid \nu_n(S,q).$$

d) Consider those q such that $q \nmid m_2$ and $q \nmid l$. Let q be an arbitrary such prime. The largest set in which $q \nmid m_2$ and $q \nmid l$ is $\mathbb{Z}$, itself. Thus $\forall n \geq 0$ and all q such that $q \nmid m_2$ and

$q \nmid l$, we have that

$$\nu_n(\mathbb{Z}, q) \mid \nu_n(S, q).$$

Since all types of primes, q, have been considered, we are in position to make a statement about $n!_S$. ¿From the above cases, we have that

$$\prod_{\substack{q|m_2\\ q\nmid l}} q^{\gamma\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{2q}\rfloor+\lfloor\frac{n}{2q^2}\rfloor+\cdots} \prod_{\substack{q|m_2\\ q|l}} q^{(2\beta+\gamma)\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{2q}\rfloor+\lfloor\frac{n}{2q^2}\rfloor+\cdots}$$

$$\prod_{\substack{q\nmid m_2\\ q|l}} q^{n\beta}\cdot\nu_n(\mathbb{Z}, q) \prod_{\substack{q\nmid m_2\\ q\nmid l}} \nu_n(\mathbb{Z}, q) \;\Bigg|\; \prod_{q\in\mathbb{P}} \nu_n(S, q) = n!_S = \alpha_n,$$

which completes the proof. □

Using Theorem 2.2(iii) ($n!|n!_S$, $\forall n \geq 0$), we can express $n!_S$ as a multiple of $n!$ (i.e., $n!_S = a \cdot n!$, $a \in \mathbb{Z}^+$). Alternatively, we can denote $n!_S$ as

$$n!_S = s(n) \cdot n!,$$

where $s : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ is determined by S. (This is a notation which will be useful later in the thesis.)

In observing Theorem 2.2(iv) and (v), it might appear that something more general could be said. For instance, if we were given $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_k$, then there would be some X such that $X|\alpha_n$, $\forall n \geq 0$, where X isn't something trivial. However the proof for the case in which $k = 2$ should perhaps imply that, as k increases, the situation becomes daunting rather quickly (indeed, the types of primes that would need to be considered doubles with each increment of k). Also, those certainties about residues in S, which arose when $k = 1$ and 2, are generally lost as k increases. To demonstrate, let $\alpha_1 = l$, $\alpha_2 = l^2 2!$, and $\alpha_3 = l^3 m_3 3!$. Let $q \neq 2, 3$ be a prime such that $q|m_3$ and $q|l$, where $\nu_1(S, q) = q^\beta$, $\nu_1(S, q) = q^{2\beta}$, and $\nu_1(S, q) = q^{3\beta+\delta}$. So, for a q-ordering of S, beginning $a_0, a_1, a_2, a_3 \dots$, we have that $w_q(a_1 - a_0) = q^\beta$, $w_q((a_2 - a_1)(a_2 - a_0)) = q^{2\beta}$, and $w_q((a_3 - a_2)(a_3 - a_1)(a_3 - a_0) = q^{3\beta+\delta}$. It must be that q^β divides each of $w_q(a_3 - a_2)$, $w_q(a_3 - a_1)$, and $w_q(a_3 - a_0)$ (else we would contradict the fact that $w_q(a_1 - a_0) = q^\beta$). Now either $w_q(a_3 - a_0) = q^\beta$ or $w_q(a_3 - a_1) = q^\beta$, since if $q^{\beta+1}$ divided both of these terms, then $q^{\beta+1}$ would divide $w_q(a_1 - a_0)$ (which is another contradiction). Assuming that $w_q(a_3 - a_0) = q^\beta$ (and with it already provided that q^β divides both $w_q(a_3 - a_2)$ and $w_q(a_3 - a_1)$), q^δ needs to be "distributed" between $w_q(a_3 - a_2)$ and $w_q(a_3 - a_1)$. Unfortunately, there are no indications as to how this distribution should be performed. Though even if the distribution was known, it's difficult to see what new information could be gleaned about the residues in S.

Perhaps there is something worthwhile to be said, but there seem to be many other more interesting problems worthy of attention.

3 !-Equivalent Subsets

Definition 3.1. S and $T \subseteq \mathbb{Z}$ are said to be !-equivalent if $\forall n \geq 0$, $n!_S = n!_T$.

Perhaps the most exciting problem associated with these factorial functions has been the search for necessary and sufficient conditions on S and $T \subseteq \mathbb{Z}$ to provide that they are !-equivalent sets. Since the presence or absense of particular residues (or groups of residues) in a set is so intimately connected with that set's factorial function, it would seem that a necessary and sufficient condition for !-equivalence would have to concern itself with relationships between residue classes. Something like prime-power equivalence (which means, for a given residue b modulo p^r, $\exists s \in S$, such that $s \equiv b(\text{mod } p^r)$ iff $\exists t \in T$, s.t. $t \equiv b(\text{mod } p^r)$) is a sufficient though not necessary condition for !-equivalence. To see this, consider $2\mathbb{Z}$ and $2\mathbb{Z}+1$. Both share the same factorial function, $n!_{2\mathbb{Z}} = n!_{2\mathbb{Z}+1} = 2^n n!$, though are clearly not prime-power equivalent. In an effort to find a condition weak enough to be implied by $n!_S = n!_T$, the conjecture below was arrived upon (but a quick definition is needed first).

Definition 3.2. $S(\text{mod } p^r) = \{0 \leq a < p^r | \exists s \in S \text{ s.t. } s \equiv a(\text{mod } p^r)\}$.

Conjecture 3.3. *Let $S, T \subseteq \mathbb{Z}$ be infinite. The following two statements are equivalent:*

i) $n!_S = n!_T$, $\forall n \geq 0$

ii) $\nu_k(S(mod\ p^r), p) = \nu_k(T(mod\ p^r), p)$, $\forall r \geq 1$, $k \geq 0$, $p \in \mathbb{P}$.

As it's presented as a conjecture, it hasn't yet been verified, at least not in the general case. However, (ii) $\Rightarrow$ (i) can be proven, as it is below (with the aid of number of lemmas).

Lemma 3.4. *If $S \subseteq \mathbb{Z}$ is infinite, then $\forall n \in \mathbb{N}$, $\exists r \in \mathbb{N}$ such that $|S(mod\ p^r)| \geq n$.*

Proof. Since S is infinite, we can select $2n$ distinct elements from S. It must be that at least n of these are positive or at least n are negative. Without loss of generality, let there be $m \geq n$ elements which are positive and collect these into a set W. (The argument for a surplus of negatives is essentially identical.) Select the greatest element in W and denote it w_{max}. Choose an $r \in \mathbb{N}$ such that $p^r > w_{max}$. So $\forall w \in W$, $0 < w < p^r$, and thus each $w \in W$ is member of a distinct residue class modulo p^r. Therefore, $|S(\text{mod } p^r)| \geq m \geq n$. □

Lemma 3.5. *If $s_i \not\equiv s_j(mod\ p^r)$ and $s_i \equiv s'_i(mod\ p^r)$, then $w_p(s_i - s_j) = w_p(s'_i - s_j)$.*

Proof. Assume instead that $w_p(s_i - s_j) \neq w_p(s'_i - s_j)$. Without loss of generality, let $w_p(s_i - s_j) > w_p(s'_i - s_j)$, where $w_p(s_i - s_j) = p^l$, $l < r$. So $s_j \equiv s_i(\text{mod } p^l)$ and $s_j \not\equiv s'_i(\text{mod } p^l)$. Thus $s_i \not\equiv s'_i(\text{mod } p^l)$, but since $l < r$ and $s_i \equiv s'_i(\text{mod } p^r)$, this is a contradiction. Therefore $w_p(s_i - s_j) = w_p(s'_i - s_j)$. □

Lemma 3.6. *Let $S = \{s_0, s_1, \dots, s_i, \dots, s_n\} \subset \mathbb{Z}$. If s_i is such that $s_i \not\equiv s_j (mod\, p^r)$, $\forall s_j \neq s_i \in S$, and $s_i \equiv s_i' (mod\, p^r)$, then for $S' = \{s_0, s_1, \dots, s_i', \dots, s_n\}$, $\nu_k(S, p) = \nu_k(S', p)$, $\forall k \geq 0$.*

Proof. Without loss of generality, let $s_0, s_1, \dots, s_i, \dots, s_n$ be a p-ordering for S.

i) Verify that $s_0, s_1, \dots, s_i', \dots, s_n$ is a p-ordering for S'.

a) Claim: $s_0, s_1, \dots, s_{i-1}$ are the first i elements in a p-ordering. Else let the first forced "deviation" occur at the ath step in the ordering (i.e., $w_p((s_a - s_{a-1}) \cdots (s_a - s_1)(s_a - s_0)) > w_p((s_b - s_{a-1}) \cdots (s_b - s_1)(s_b - s_0))$, where $b > a$). If $s_b \neq s_i'$, then $s_0, s_1, \dots, s_i, \dots, s_n$ cannot be a valid p-ordering for S (since $w_p((s_a - s_{a-1}) \cdots (s_a - s_0)) > w_p((s_b - s_{a-1}) \cdots (s_b - s_0))$, where $b > a$).

If $s_b = s_i'$,

$$w_p((s_a - s_{a-1}) \cdots (s_a - s_1)(s_a - s_0)) > w_p((s_i' - s_{a-1}) \cdots (s_i' - s_1)(s_i' - s_0))$$
$$> w_p((s_i - s_{a-1}) \cdots (s_i - s_1)(s_i - s_0)).$$

So again, $s_0, s_1, \dots, s_i, \dots, s_n$ cannot be a valid p-ordering for S. Thus $s_0, s_1, \dots, s_{i-1}$ are the first i elements in a p-ordering.

b) Claim: s_i' is an acceptable next element in a p-ordering beginning like the above. Else $\exists\ i < c \leq n$ such that

$$w_p((s_c - s_{i-1}) \cdots (s_c - s_1)(s_c - s_0)) < w_p((s_i' - s_{a-1}) \cdots (s_i' - s_1)(s_i' - s_0))$$
$$< w_p((s_i - s_{a-1}) \cdots (s_i - s_1)(s_i - s_0)).$$

So again, $s_0, s_1, \dots, s_i, \dots, s_n$ cannot be a valid p-ordering for S. Thus s_i' is an acceptable next element.

c) Claim: $s_{i+1}, s_{i+2}, \dots, s_n$ finishes the p-ordering. Otherwise, let the first forced deviation occur at the dth step. So $w_p((s_d - s_{d-1}) \cdots (s_d - s_1)(s_d - s_0)) > w_p((s_e - s_{d-1}) \cdots (s_e - s_1)(s_e - s_0))$, where $e > d$. But

$$w_p((s_e - s_{d-1}) \cdots (s_e - s_i') \cdots (s_e - s_1)(s_e - s_0)) <$$
$$w_p((s_d - s_{d-1}) \cdots (s_d - s_i') \cdots (s_d - s_1)(s_d - s_0))$$

$$w_p((s_e - s_{d-1}) \cdots (s_e - s_i) \cdots (s_e - s_1)(s_e - s_0)) <$$
$$w_p((s_d - s_{d-1}) \cdots (s_d - s_i) \cdots (s_d - s_1)(s_d - s_0)).$$

So again, $s_0, s_1, \dots, s_i, \dots, s_n$ cannot be a valid p-ordering for S. Thus $s_0, s_1, \dots, s_i', \dots, s_n$ is a p-ordering for S'.

ii) Verify that $\nu_k(S, p) = \nu_k(S', p)$, $\forall k \geq 0$. If $k > n$, then $\nu_k(S', p) = 0 = \nu_k(S, p)$. If $k \leq n$, then

$$\nu_k(S', p) = w_p((s_k - s_{k-1}) \cdots (s_k - s_i') \cdots (s_k - s_1)(s_k - s_0))$$

$$= w_p((s_k - s_{k-1})\cdots(s_k - s_i)\cdots(s_k - s_1)(s_k - s_0)) = \nu_k(S,p).$$

This completes the proof. □

Theorem 3.7. *Let $S, T \subseteq \mathbb{Z}$ be infinite. If $\nu_k(S(mod\ p^r), p) = \nu_k(T(mod\ p^r), p)$, $\forall r \geq 1$, $k \geq 0$, $p \in \mathbb{P}$, then $n!_S = n!_T$, $\forall n \in \mathbb{N}$.*

Proof. Let $n \geq 0$, $p \in \mathbb{P}$ be arbitrary. By Lemma 3.4, $\exists\ l \in \mathbb{N}$ such that $\left|S(\text{mod } p^l)\right| > n$. And from the premise, we have that $\left|T(\text{mod } p^l)\right| = \left|S(\text{mod } p^l)\right| > n$. Now if $S(\text{mod } p^l) = \{r_0, r_1, \ldots, r_m\}$ (where $m \geq n$), then $\exists A = \{a_0, a_1, \ldots, a_m\} \subseteq S$ such that

$$a_0 \equiv r_0(\text{mod } p^l)$$

$$a_1 \equiv r_1(\text{mod } p^l)$$

$$\vdots$$

$$a_m \equiv r_m(\text{mod } p^l).$$

By applying Lemma 3.6, we get that $\nu_k(S(\text{mod } p^l), p) = \nu_k(A,p)$, $\forall k \geq 0$. So specifically, $\nu_n(S(\text{mod } p^l), p) = \nu_n(A,p)$ and since $A \subseteq S$, $\nu_k(S,p) \mid \nu_k(A,p)$. Let $\nu_k(A,p) = p^\gamma$.

Similarly, if $T(\text{mod } p^l) = \{u_0, u_1, \ldots, u_m\}$, then $\exists B = \{b_0, b_1, \ldots, b_m\} \subseteq T$ such that

$$b_0 \equiv u_0(\text{mod } p^l)$$

$$b_1 \equiv u_1(\text{mod } p^l)$$

$$\vdots$$

$$b_m \equiv u_m(\text{mod } p^l).$$

Here $\nu_n(T(\text{mod } p^l), p) = \nu_n(B,p)$, and since $B \subseteq T$, $\nu_k(T,p) \mid \nu_k(B,p)$. From our initial assumption, we have that $\nu_k(B,p) = \nu_n(T(\text{mod } p^l), p) = \nu_n(S(\text{mod } p^l), p) = \nu_n(A,p) = p^\gamma$. There are two cases to consider.

a) $\gamma < l$. Let $a_0, a_1, \ldots, a_n$ be the first n-steps in a p-ordering for A. Denote $A' = \{a_0, a_1, \ldots, a_n\}$, where obviously $\nu_n(A', p) = \nu_n(A,p)$. Now let $s_0, s_1, \ldots, s_n$ be the first n-steps in a p-ordering for S. Again denote $S' = \{s_0, s_1, \ldots, s_n\}$, where $\nu_n(S', p) = \nu_n(S,p)$.

Claim: $s_i \not\equiv s_j(\text{mod } p^l)$, $\forall i \neq j$.

Now assume that there are $s_i, s_j \in S'$ (where $j > i$) such that $s_i \equiv s_j(\text{mod } p^l)$. So $\nu_j(S', p) = w_p((s_j - s_{j-1})\cdots(s_j - s_i)\cdots(s_j - s_1)(s_j - s_0)) \geq p^l$. Thus $p^l \mid \nu_j(S', p) \mid$

$\nu_n(S', p) = \nu_n(S, p)$. So since $\nu_n(S, p) \mid \nu_n(A, p)$, $p^l \mid \nu_n(A, p) = p^\gamma$. However, $\gamma < l$, which is a contradiction. So it must be that $s_i \not\equiv s_j (\text{mod } p^l)$, $\forall i \neq j$.

Given that $s_i \not\equiv s_j (\text{mod } p^l)$, $\forall i \neq j$, we have that

$$s_0 \equiv r'_0 (\text{mod } p^l)$$

$$s_1 \equiv r'_1 (\text{mod } p^l)$$

$$\vdots$$

$$s_n \equiv r'_n (\text{mod } p^l)'$$

where $\{r'_0, r'_1, \ldots, r'_n\} = R' \subseteq S(\text{mod } p^l)$, with the r_i's distinct. By Lemma 3.6, $\nu_n(R', p) = \nu_n(S', p) = \nu_n(S, p)$ and since $R' \subseteq S(\text{mod } p^l)$, $\nu_n(A, p) = \nu_n(S(\text{mod } p^l), p) \mid \nu_n(R', p) = \nu_n(S, p)$. Therefore, along with $\nu_n(S, p) \mid \nu_n(A, p)$ from above, $\nu_n(S, p) = \nu_n(A, p) = \nu_n(S(\text{mod } p^l), p)$. Using an analogous argument, we have that $\nu_n(T, p) = \nu_n(B, p) = \nu_n(T(\text{mod } p^l), p)$. Thus when $\gamma < l$, we have that $\nu_n(S, p) = \nu_n(S(\text{mod } p^l), p) = \nu_n(T(\text{mod } p^l), p) = \nu_n(T, p)$.

b) $\gamma \geq l$: Consider the set $S(\text{mod } p^{\gamma+1})$. Again if $S(\text{mod } p^{\gamma+1}) = \{q_0, q_1, \ldots, q_w\}$ (where $w \geq n$), then $\exists\, C = \{c_0, c_1, \ldots, c_w\} \subseteq S$ such that

$$c_0 \equiv q_0 (\text{mod } p^{\gamma+1})$$

$$c_1 \equiv q_1 (\text{mod } p^{\gamma+1})$$

$$\vdots$$

$$c_w \equiv q_w (\text{mod } p^{\gamma+1}).$$

So $\nu_n(S, p) \mid \nu_n(C, p) = \nu_n(S(\text{mod } p^{\gamma+1}), p)$. Again let S' be defined as above.

Claim: $s_i \not\equiv s_j (\text{mod } p^{\gamma+1})$, $\forall i \neq j$.

Again assume there are $s_i, s_j \in S'$ (where $j > i$) such that $s_i \equiv s_j (\text{mod } p^{\gamma+1})$. So $\nu_j(S', p) = w_p((s_j - s_{j-1}) \cdots (s_j - s_i) \cdots (s_j - s_1)(s_j - s_0)) \geq p^{\gamma+1}$. Thus $p^{\gamma+1} \mid \nu_j(S', p) \mid \nu_n(S', p) = \nu_n(S, p)$. So, since $\nu_n(S, p) \mid \nu_n(A, p)$, $p^{\gamma+1} \mid \nu_n(A, p) = p^\gamma$. However, this is a contradiction. So it must be that $s_i \not\equiv s_j (\text{mod } p^{\gamma+1})$, $\forall i \neq j$.

Given that $s_i \not\equiv s_j (\text{mod } p^{\gamma+1})$, $\forall i \neq j$, we have that

$$s_0 \equiv v'_0 (\text{mod } p^{\gamma+1})$$

$$s_1 \equiv v_1'(\text{mod } p^{\gamma+1})$$

$$\vdots$$

$$s_n \equiv v_n'(\text{mod } p^{\gamma+1})'$$

where $\{v_0', v_1', \ldots, v_n'\} = V' \subseteq S(\text{mod } p^{\gamma+1})$, with the v_i's distinct. By Lemma 3.6, $\nu_n(V', p) = \nu_n(S', p) = \nu_n(S, p)$ and since $V' \subseteq S(\text{mod } p^{\gamma+1})$, $\nu_n(C, p) = \nu_n(S(\text{mod } p^{\gamma+1}), p) \mid \nu_n(V', p) = \nu_n(S, p)$. Therefore, along with $\nu_n(S, p) \mid \nu_n(C, p)$ from above, $\nu_n(S, p) = \nu_n(C, p) = \nu_n(S(\text{mod } p^{\gamma+1}), p)$. Again using a similar argument, we have that $\nu_n(T, p) = \nu_n(T(\text{mod } p^{\gamma+1}), p)$. Thus when $\gamma \geq l$, $\nu_n(S, p) = \nu_n(S(\text{mod } p^{\gamma+1}), p) = \nu_n(T(\text{mod } p^{\gamma+1}), p) = \nu_n(T, p)$.

With both cases considered, we have that $\nu_n(S, p) = \nu_n(T, p)$. And since $n \geq 0$ and $p \in \mathbb{P}$ were both arbitrary, $n!_S = n!_T$, $\forall n \geq 0$. This completes the proof. □

Again this only proves the conjecture in one direction; however if one of our sets is $\mathbb{Z}$, itself, the conjecture does hold.

Theorem 3.8. *Let S be infinite. The following two statements are equivalent:*

i) $n!_S = n!$, $\forall n \geq 0$

ii) $\nu_k(S(mod\ p^r), p) = \nu_k(\mathbb{Z}(mod\ p^r), p)$, $\forall r \geq 1$, $k \geq 0$, $p \in \mathbb{P}$.

Proof. (ii) ⇒ (i): This has already been proven generally.

(i) ⇒ (ii): Let it be that $n!_S = n!$, $\forall n \in \mathbb{N}$. Suppose instead that $\exists r \geq 1$, $k \geq 0$, $p \in \mathbb{P}$ s.t. $\nu_k(S(\text{mod } p^r), p) = \nu_k(\mathbb{Z}(\text{mod } p^r), p)$. Since $\mathbb{Z}(\text{mod } p^r))$ contains all residues modulo p^r, it must be that there is an $0 \leq i < p^r$ such that $\forall s \in S$, $s \not\equiv i(\text{mod } p^r))$. So $S \subseteq T = \{z \in \mathbb{Z} \mid z \not\equiv i(\text{mod } p^r)\}$. From above, we have that $0, 1, 2, 3, \ldots$ is a valid p-ordering for $\mathbb{Z}$. Since $0, 1, 2, \ldots, i-1 \in T$, it should be obvious that the sequence, $0, 1, 2, \ldots, i-1$, is valid for the first $i-1$ steps in a p-ordering for T. However since $i \notin R$, the ordering cannot continue without alteration.

Claim: There is a p-ordering for T such that $t_0, t_1, t_2, \ldots, t_{p^r-2}$ are all in the interval $[0, p^r - 1]$.

See Appendix for proof of claim (Notes A.4).

Given the above p-ordering, a beginning in which all integers in the interval $[0, p^r - 1]$ except i have been used, we must minimize $w_p((t_{p^r-1} - (p^r-1))(t_{p^r-1} - (p^r-2)) \cdots (t_{p^r-1} - (i+1))(t_{p^r-1} - (i-1)) \cdots (t_{p^r-1} - 1)(t_{p^r-1} - 0))$ for the $(p^r - 1)$th step. Since $\nexists t \in T$ such that $t \equiv i(\text{mod } p^r)$, any choice for t_{p^r-1} must be congruent to some integer in the interval $[0, p^r - 1]$ modulo p^r.

Now

$$w_p(p!) = w_p((p^r - (p^r - 1))(p^r - (p^r - 2)) \cdots (p^r - i) \cdots (p^r - 1)(p^r - 0))$$

$$= p^r \cdot w_p((p^r - (p^r - 1))(p^r - (p^r - 2)) \cdots (p^r - (i+1))(p^r - (i-1)) \cdots (p^r - 1))$$

$$= p^r \cdot w_p((p^r - 1 - (p^r - 2))(p^r - 1 - (p^r - 3)) \cdots (p^r - 1 - i) \cdots (p^r - 1))$$

$$= p^r \cdot w_p((p^r - 1)!).$$

And since $w_p(p!) \leq w_p((t_{p^r-1} - (p^r - 1))(t_{p^r-1} - (p^r - 2)) \cdots (t_{p^r-1} - i) \cdots (t_{p^r-1} - 1)(t_{p^r-1} - 0))$, we have that

$$p^r \cdot w_p((p^r - 1)!) \leq w_p((t_{p^r-1} - (p^r - 1))(t_{p^r-1} - (p^r - 2)) \cdots (t_{p^r-1} - i) \cdots (t_{p^r-1} - 1)(t_{p^r-1} - 0))$$

$$p^r \cdot \nu_{p^r-1}(\mathbb{Z}, p) \leq w_p(t_{p^r-1} - i) \cdot w_p((t_{p^r-1} - (p^r - 1))(t_{p^r-1} - (p^r - 2)) \cdots (t_{p^r-1} - (i+1))(t_{p^r-1} - (i-1)) \cdots (t_{p^r-1} - 1)(t_{p^r-1} - 0))$$

$$p^r \cdot \nu_{p^r-1}(\mathbb{Z}, p) \leq w_p(t_{p^r-1} - i) \cdot \nu_{p^r-1}(T, p).$$

And since it has been assumed that $n!_S = n!_T = n!$, $\nu_{p^r-1}(\mathbb{Z}, p) = \nu_{p^r-1}(T, p)$. So

$$p^r \leq w_p(t_{p^r-1} - i).$$

But since $\nexists t \in T$ such that $t \equiv i (\text{mod } p^r)$ and with $t_{p^r-1} \in T$, we have a contradiction. Therefore (ii) must hold. This completes the proof. □

4 Results Concerning Generalized Binomial Coefficients

¿From above, notice that $\binom{n}{k}_{2\mathbb{Z}} = \binom{n}{k}_{\mathbb{Z}} = \binom{n}{k}$ (i.e., the $\binom{n}{k}_E$ are merely the binomial coefficients we are already familar with). It would seem to be worthwhile to determine for which subsets, S, $\binom{n}{k}_S = \binom{n}{k}$. More generally, we would like to determine conditions on subsets S and T of $\mathbb{Z}$ which provide that $\binom{n}{k}_S = \binom{n}{k}_T$. To this effect, we have the following theorem.

Theorem 4.1. *Let S and T be subsets of $\mathbb{Z}$. The following two statements are equivalent:*

i) $\binom{n}{k}_S = \binom{n}{k}_T$, for all $n \geq k \in \mathbb{Z}$.

ii) Let $1!_S = l$ and $1!_T = l'$. Then $n!_S = l^n \cdot m_n \cdot n!$ and $n!_T = (l')^n \cdot m_n \cdot n!$, for all $n \in \mathbb{Z}^+$ (where $m_n \in \mathbb{Z}^+$ is dependent on n and S or T).

Proof. (i) ⇒ (ii) Assume that the property described in (i) holds for S and T. By employing a previously introduced notation ($n!_S = s(n) \cdot n!$, where $s : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ is dependent on S), we have that for $n \geq k$:

$$\binom{n}{k}_S = \binom{n}{k}_T \;\Rightarrow$$

$$\frac{n!_S}{k!_S(n-k)!_S} = \frac{n!_T}{k!_T(n-k)!_T} \;\Rightarrow$$

$$\frac{s(n)n!}{s(k)k! \cdot s(n-k)(n-k)!} = \frac{t(n)n!}{t(k)k! \cdot t(n-k)(n-k)!} \;\Rightarrow$$

$$\frac{s(n)}{s(k) \cdot s(n-k)} = \frac{t(n)}{t(k) \cdot t(n-k)} \;\Rightarrow$$

$$s(n) \cdot t(k)t(n-k) = t(n) \cdot s(k)s(n-k).$$

By substituting, we get that $s(a+b) \cdot t(a)t(b) = t(a+b) \cdot s(a)s(b)$, for all $a, b \in \mathbb{Z}^+$. Now given that $s(1) = l$ and $t(1) = l'$, we have from a previous result that $s(i) = l^i \cdot m_i$ and $t(i) = (l')^i \cdot m'_i$. Now, we need to show that $m_i = m'_i$. We use induction. The initial case, $i = 1$, has already been provided, as $m_1 = m'_1 = 1$. Assume that the property holds for $i = j$; so we must show that it holds when $i = j+1$. Using the above formula, we have that:

$$s(j+1) \cdot t(j)t(1) = t(j+1) \cdot s(j)s(1) \;\Rightarrow$$

$$l^{j+1}m_{j+1} \cdot (l')^j m_j \cdot l' = (l')^{j+1}m'_{j+1} \cdot l^j m_j \cdot l \;\Rightarrow$$

$$l^{j+1}(l')^{j+1}m_j \cdot m_{j+1} = l^{j+1}(l')^{j+1}m_j \cdot m'_{j+1} \;\Rightarrow$$

$$m_{j+1} = m'_{j+1}.$$

So we have that $n!_S = l^n \cdot m_n \cdot n!$ and $n!_T = (l')^n \cdot m_n \cdot n!$, for all $n \in \mathbb{Z}^+$.

(ii) ⇒ (i) Let S and T be such that $n!_S = l^n \cdot m_n \cdot n!$ and $n!_T = (l')^n \cdot m_n \cdot n!$, for all $n \in \mathbb{Z}^+$ (where $1!_S = l$, $1!_T = l'$). Then, for an arbitrary $n, k \in \mathbb{N}$ ($n \geq k$),

$$\binom{n}{k}_S = \frac{n!_S}{k!_S(n-k)!_S} = \frac{l^n m_n n!}{l^k m_k k! \cdot l^{n-k} m_{n-k}(n-k)!}$$

$$= \frac{l^n \cdot m_n n!}{l^n \cdot m_k m_{n-k} k!(n-k)!} = \frac{m_n n!}{m_k m_{n-k} k!(n-k)!},$$

and similarly,

$$\binom{n}{k}_T = \frac{n!_T}{k!_T(n-k)!_T} = \frac{(l')^n m_n n!}{(l')^k m_k k! \cdot (l')^{n-k} m_{n-k}(n-k)!}$$

$$= \frac{(l')^n \cdot m_n n!}{(l')^n \cdot m_k m_{n-k} k!(n-k)!} = \frac{m_n n!}{m_k m_{n-k} k!(n-k)!}.$$

So, since n and k are arbitrary in $\mathbb{N}$, we have that $\binom{n}{k}_S = \binom{n}{k}_T$, for all $n \geq k \in \mathbb{Z}$. □

While this is a mildly interesting result in itself, it also gives us the following corollary.

Corollary 4.2. *Let S be a subset of $\mathbb{Z}$. The following statements are equivalent:*

i) $\binom{n}{k}_S = \binom{n}{k}$*, for all* $n \geq k \in \mathbb{Z}$.

ii) Let $1!_S = l$*. Then* $n!_S = l^n \cdot n!$.

iii) S *is* $!$*-equivalent to* $l\mathbb{Z} + b$*, where* $b \in \mathbb{Z}$.

Proof. (i) ⇒ (ii) This is merely an application of the above theorem (letting $T = \mathbb{Z}$). Since $n!_{\mathbb{Z}} = n!$, $m_n = 1$ for all $n \in \mathbb{N}$, hence the result in (ii).

(ii) ⇒ (iii) This is rather easy to show as we know from Bhargava ([4][Example 17]) that $n!_{l\mathbb{Z}+b} = l^n \cdot n!$. Thus $n!_{l\mathbb{Z}+b} = n!_S$, $\forall n \in \mathbb{N}$, meaning S and $l\mathbb{Z} + b$ are !- equivalent.

(iii) ⇒ (i) Since S and $l\mathbb{Z} + b$ are !-equivalent we have that $n!_S = n!_{l\mathbb{Z}+b} = l^n \cdot n!$. So $m'_n = 1 = m_n$, $\forall n \in \mathbb{N}$, again leaving this proof to be just an application of the above theorem. □

Pascal's triangle has been an important tool for determining (or at least visualizing) properties concerning the binomial coefficients. Given our improved grasp of the generalized coefficients, it would seem that the construction of a "generalized" Pascal's triangle would be a useful endeavor. The triangle can be defined in the obvious way:

$$\begin{matrix} \binom{0}{0}_S \\ \binom{1}{0}_S \binom{1}{1}_S \\ \binom{2}{0}_S \binom{2}{1}_S \binom{2}{2}_S \\ \binom{3}{0}_S \binom{3}{1}_S \binom{3}{2}_S \binom{3}{3}_S . \\ \vdots \end{matrix}$$

Since we've stipulated that $0!_S = 1$ for all subsets, $\binom{n}{0}_S = \binom{n}{n}_S = 1$ for all n. This is in some ways unfortunate, since it restricts Pascal's Identity ($\binom{n}{i}_S + \binom{n}{i+1}_S = \binom{n+1}{i+1}_S$, for $n, i \geq 0$) to only those subsets, S, such that $\binom{n}{k}_S = \binom{n}{k}$. The following lemma makes this evident.

Lemma 4.3. *The identity,* $\binom{n}{i}_S + \binom{n}{i+1}_S = \binom{n+1}{i+1}_S$*, holds only for those subsets, S, for which* $\binom{n}{i}_S = \binom{n}{i}_{\mathbb{Z}}$, $\forall n, i \geq 0$.

Proof. Let Pascal's Identity hold for the binomial coefficients of a set $S \subseteq \mathbb{Z}$. Now suppose that $\exists n, i \in \mathbb{N}$ such that $\binom{n}{i}_S \neq \binom{n}{i}_\mathbb{Z}$. Let a be the least integer such that $\exists b \in \mathbb{N}$ where $\binom{a}{b}_S \neq \binom{a}{b}_\mathbb{Z}$. Since $\binom{n}{0}_S = \binom{n}{n}_S = 1$ for all $S \subseteq \mathbb{Z}$, $b \neq 0$ and $a \neq b$. So both $\binom{a-1}{b-1}_S$ and $\binom{a-1}{b}_S$ are well-defined. And since $a-1 < a$, $\binom{a-1}{b-1}_S = \binom{a-1}{b-1}_\mathbb{Z}$ and $\binom{a-1}{b}_S = \binom{a-1}{b}_\mathbb{Z}$. Since Pascal's Identity holds,

$$\binom{a}{b}_S = \binom{a-1}{b-1}_S + \binom{a-1}{b}_S$$

$$= \binom{a-1}{b-1}_\mathbb{Z} + \binom{a-1}{b}_\mathbb{Z} = \binom{a}{b}_\mathbb{Z}.$$

But this is a contradiction. Therefore, it must be that $\binom{n}{i}_S = \binom{n}{i}_\mathbb{Z}$, $\forall n, i \geq 0$. □

Additionally, there doesn't seem to be any obvious way to "tweak" the property so that it might hold generally. Again, this is unfortunate since many of the interesting properties of Pascal's Triangle are founded upon this rule. Despite this, there is at least one property of Pascal's Triangle which remains valid.

Theorem 4.4. *Let $n, 0 < k < n \in \mathbb{N}$. On the generalized Pascal's Triangle for a subset S, the product of the six entries surrounding $\binom{n}{k}_S$ is a perfect square.*

Proof. To prove this, we must show that

$$\binom{n-1}{k-1}_S \cdot \binom{n-1}{k}_S \cdot \binom{n}{k-1}_S \cdot \binom{n}{k+1}_S \cdot \binom{n+1}{k}_S \cdot \binom{n+1}{k+1}_S = a^2,$$

where $a \in \mathbb{Z}$. So

$$\binom{n-1}{k-1}_S \cdot \binom{n-1}{k}_S \cdot \binom{n}{k-1}_S \cdot \binom{n}{k+1}_S \cdot \binom{n+1}{k}_S \cdot \binom{n+1}{k+1}_S =$$

$$\frac{s(n-1)(n-1)!}{s(k-1)(k-1)!s(n-k)(n-k)!} \cdot \frac{s(n-1)(n-1)!}{s(k)k!s(n-k-1)(n-k-1)!} \cdot$$

$$\frac{s(n)n!}{s(k-1)(k-1)!s(n-k+1)(n-k+1)!} \cdot \frac{s(n)n!}{s(k+1)(k+1)!s(n-k-1)(n-k-1)!} \cdot$$

$$\frac{s(n+1)(n+1)!}{s(k)k!s(n-k+1)(n-k+1)!} \cdot \frac{s(n+1)(n+1)!}{s(k+1)(k+1)!s(n-k)(n-k)!}$$

$$= \frac{s(n-1)}{s(k-1)s(n-k)} \cdot \frac{s(n-1)}{s(k)s(n-k-1)} \cdot \frac{s(n)}{s(k-1)s(n-k+1)} \cdot$$

$$\frac{s(n)}{s(k+1)s(n-k-1)} \cdot \frac{s(n+1)}{s(k)s(n-k+1)} \cdot \frac{s(n+1)}{s(k+1)s(n-k)} \cdot$$

$$\frac{(n-1)!}{(k-1)!(n-k)!} \cdot \frac{(n-1)!}{k!(n-k-1)!} \cdot \frac{n!}{(k-1)!(n-k+1)!} \cdot$$

$$\frac{n!}{(k+1)!(n-k-1)!} \cdot \frac{(n+1)!}{k!(n-k+1)!} \cdot \frac{(n+1)!}{(k+1)!(n-k)!}$$

$$= (\frac{s(n-1)s(n)s(n+1)}{s(k-1)s(k)s(k+1)s(n-k-1)s(n-k)s(n-k+1)})^2 \cdot b^2$$

$$= (b \cdot \frac{s(n-1)s(n)s(n+1)}{s(k-1)s(k)s(k+1)s(n-k-1)s(n-k)s(n-k+1)})^2 = a^2.$$

□

References

[1] M. Bhargava, Generalized factorials and fixed divisors over subsets of a Dedekind domain, *J. Number Theory* **72**(1998), 67–75.

[2] M. Bhargava, Congruence preservation and polynomial functions from Z_n to Z_m, *Discrete Math.* **173**(1997), 15–21.

[3] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490**(1997), 101–127.

[4] M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly.* **107**(2000), 783-799.

[5] M. Bhargava and K.S. Kedlaya, Continuous functions on compact subsets of local fields, *Acta Arith.* **91**(1999), 191–198.

[6] P.-J. Cahen and J.-L. Chabert, "Integer Valued-Polynomials," Amer. Math. Soc. Surveys and Monographs, **58**(1997), American Mathematical Society, Providence.

[7] D.S. Dummit and R.M. Foote, *Abstract Algebra, 2nd ed.*. Upper Saddle River, N.J.: Prentice Hall, 1999.

[8] C. Long, Pascal's triangle, difference tables and arithmetic sequences of order N, *College Math. Journal* **15**(1984), 290–298.

A Appendix

Notes A.1. To verify the p-ordering we use induction. We can choose a_0 arbitrarily, so choose c.

$P(1)$: Now since $q \nmid (d-c)$, d minimizes $w_q(a_1-c)$. So we may justifiably choose $a_1 = d$.

$P(n) \to P(n+1)$: n may be even or odd, so we must consider both cases.

Let n be even. So the q-ordering (up to the nth step) is $c, d, \dots, \frac{n}{2}q^\gamma + c$. We need to show that $\frac{n}{2}q^\gamma + d$ is an adequate choice for a_{n+1}, by showing that it minimizes $w_p((a_{n+1} - \frac{n}{2}q^\gamma - c)\cdots(a_{n+1}-d)(a_{n+1}-c))$. Now a_{n+1} must be of the form $vq^\gamma + c$ or $uq^\gamma + d$. If $a_{n+1} = vq^\gamma + c$,

$$w_p((vq^\gamma + c - \frac{n}{2}q^\gamma - c)\cdots(vq^\gamma + c - d)(vq^\gamma + c - c)) =$$
$$w_p((vq^\gamma + c - \frac{n}{2}q^\gamma - c)\cdots(vq^\gamma + c - q^\gamma - c)(vq^\gamma + c - c)),$$

since $w_p(vq^\gamma + c - iq^\gamma - d) = 1$, $\forall i \in \mathbb{Z}$. Continuing,

$$w_p((vq^\gamma - \frac{n}{2}q^\gamma)\cdots(vq^\gamma - q^\gamma)(vq^\gamma)) = w_p(v(v-1)(v-2)\cdots(v-\frac{n}{2})\cdot q^{\frac{\gamma/(n+2)}{2}})$$

$$= q^{(\frac{\gamma/(n+2)}{2})} \cdot w_p(v(v-1)(v-2)\cdots(v-\frac{n}{2})).$$

This is minimized by $v = \frac{n+2}{2}$, so here we have $q^{(\frac{\gamma/(n+2)}{2})} \cdot w_p((\frac{n+2}{2})!)$.

Now if a_{n+1} is of the form $uq^\gamma + d$,

$$w_p((uq^\gamma + d - \frac{n}{2}q^\gamma - c)\cdots(uq^\gamma + d - d)(uq^\gamma + d - c)) =$$
$$w_p((uq^\gamma + d - \frac{n-2}{2}q^\gamma - d)\cdots(uq^\gamma + d - q^\gamma - d)(uq^\gamma + d - d)) =$$
$$w_p((uq^\gamma - \frac{n-2}{2}q^\gamma)\cdots(uq^\gamma - q^\gamma)(uq^\gamma)) =$$
$$w_p(u(u-1)(u-2)\cdots(u-\frac{n-2}{2})\cdot q^{\frac{\gamma/n}{2}}) =$$
$$q^{(\frac{\gamma/n}{2})} \cdot w_p(u(u-1)(u-2)\cdots(u-\frac{n-2}{2})).$$

This is minimized by $u = \frac{n}{2}$, so here we have $q^{(\frac{\gamma/n}{2})} \cdot w_p((\frac{n-2}{2})!)$. This is clearly less than $q^{(\frac{\gamma/(n+2)}{2})} \cdot w_p((\frac{n+2}{2})!)$, so the best choice for a_{n+1} is $\frac{n}{2}q^\gamma + d$.

Let n be odd. Here we would need to show that $\frac{n+1}{2}q^\gamma + c$ is an adequate choice for a_{n+1}. This can be shown using a proof analogous to the one above, so let it be accepted without explicit demonstration. With this, the inductive proof is complete. Thus $c, d, q^\gamma + c, q^\gamma + d, 2q^\gamma + c, 2q^\gamma + d, \dots$ is a valid q-ordering for T.

Notes A.2. It should be fairly apparent that $w_q((a_n - a_{n-1}) \cdots (a_n - a_1)(a_n - a_0)) = q^{\alpha}$, where

$$\alpha = |\{a_i \equiv a_n (\text{mod } q) | 0 \leq i < n\}| + \left|\{a_i \equiv a_n (\text{mod } q^2) | 0 \leq i < n\}\right| \\ + \left|\{a_i \equiv a_n (\text{mod } q^3) | 0 \leq i < n\}\right| + \cdots .$$

And since $|\{i \equiv n(\text{mod } q^r) | 0 \leq i < n\}| = \lfloor \frac{n}{q^r} \rfloor$, we have that $w_q(\frac{n}{2}!) = q^{\lfloor \frac{n}{2q} \rfloor + \lfloor \frac{n}{2q^2} \rfloor + \lfloor \frac{n}{2q^3} \rfloor + \cdots}$.

Notes A.3. Let n be odd. Assume instead that $\lfloor \frac{n}{2q^r} \rfloor \neq \lfloor \frac{n-1}{2q^r} \rfloor$. Thus $\exists m \in \mathbb{Z}$ such that

$$\frac{n-1}{2q^r} < m \leq \frac{n}{2q^r}$$

$$n - 1 < 2q^r m \leq n$$

So it must be that $n = 2q^r m$, but n is odd, which is a contradiction. Therefore $\lfloor \frac{n}{2q^r} \rfloor = \lfloor \frac{n-1}{2q^r} \rfloor$.

Notes A.4. The following constuction is a valid p-ordering to the $(p^r - 2)$nd step: Let the first $i - 1$ steps be determined as above. (Note that if $i = p^r - 1$, then we already have a p-ordering to the $(p^r - 2)$nd step, so no further construction is needed.)

Let p^{u_1} be the greatest power of p less than $p^r - i$. Let $i \equiv b_{u_1} (\text{mod } p^{u_1})$. Then the ith element will be $p^r - p^{u_1} + b_{u_1}$. For $i < j < p^r - p^{u_1} + b_{u_1}$, the jth element will be j.

Let p^{u_2} be the greatest power of p less than $p^r - (p^r - p^{u_1} + b_{u_1}) = p^{u_1} - b_{u_1}$. Let $i \equiv b_{u_2} (\text{mod } p^{u_2})$. Then the $(p^r - p^{u_1} + b_{u_1})$th element will be $p^r - p^{u_2} + b_{u_2}$. For $p^r - p^{u_1} + b_{u_1} < j < p^r - p^{u_2} + b_{u_2}$, the jth element will be j.

$$\vdots$$

Let $p^{u_{k+1}}$ be the greatest power of p less than $p^r - (p^r - p^{u_k} + b_{u_k}) = p^{u_k} - b_{u_k}$. Let $i \equiv b_{u_{k+1}} (\text{mod } p^{u_{k+1}})$. Then the $(p^r - p^{u_k} + b_{u_k})$th element will be $p^r - p^{u_{k+1}} + b_{u_{k+1}}$. For $p^r - p^{u_k} + b_{u_k} < j < p^r - p^{u_{k+1}} + b_{u_{k+1}}$, the jth element will be j.

$$\vdots$$

When $p^r - (p^r - p^{u_l} + b_{u_l}) = p^{u_l} - b_{u_l} < p$, we have that for $p^r - p^{u_l} + b_{u_l} \leq j < p^r - 1$, the jth element is $j + 1$. And this completes the p-ordering to the $(p^r - 2)$nd step.

The acceptability of the first $i - 1$ steps has already been noted. Now induction should be done on j to establish the rest of the claim.

$P(i)$: We begin with the ith element. We may assume that $i \neq p^r - 1$, since we are then already provided a p-ordering to the (p^t-2)nd step (namely, $0, 1, 2, \ldots, i-1$). So in choosing the ith element, we are looking to minimize $w_p((a_i-(i-1))(a_i-(i-2))\cdots(a_i-1)(a_i-0))$. There are two cases to consider–when $u_1 > 0$ and when $u_1 = 0$.

Let $u_1 > 0$. Consider the element $p^r - p^{u_1} + b_{u_1}$. Now $w_p((p^r - p^{u_1} + b_{u_1} - (i-1))(p^r - p^{u_1} + b_{u_1} - (i-2))\cdots(p^r - p^{u_1} + b_{u_1} - 1)(p^r - p^{u_1} + b_{u_1} - 0)) = p^{\alpha}$, where $\alpha = |\{n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p) \mid 0 \leq n < i\}| + \big|\{n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^2) \mid 0 \leq n < i\}\big| + \cdots + \big|\{n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^{r-1}) \mid 0 \leq n < i\}\big|$. (No other terms are needed since there is no n in our interval such that $n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^r)$.)

So for p^v where $u_1 < v < r$, $p^r - p^v \leq i, p^r - p^{u_1} + b_{u_1} < p^r$; thus $\lfloor \frac{p^r - p^{u_1} + b_{u_1}}{p^v} \rfloor = \lfloor \frac{i}{p^v} \rfloor$. Now $|\{n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^v) \mid 0 \leq n < i\}| \leq \lfloor \frac{p^r - p^{u_1} + b_{u_1}}{p^v} \rfloor$, so

$$|\{n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^v) \mid 0 \leq n < i\}| \leq \lfloor \frac{i}{p^v} \rfloor.$$

For p^y where $1 \leq y \leq u_1$, $i \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^y)$. Thus

$$|\{n \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^y) \mid 0 \leq n < i\}| = |\{n \equiv i (\text{mod } p^y) \mid 0 \leq n < i\}| = \lfloor \frac{i}{p^v} \rfloor.$$

Together we have that $p^{\alpha} \leq p^{\lfloor \frac{i}{p} \rfloor + \lfloor \frac{i}{p^2} \rfloor + \cdots + \lfloor \frac{i}{p^{r-1}} \rfloor} = \nu_i(\mathbb{Z}, p)$. And since $\nu_i(\mathbb{Z}, p) | p^{\alpha}$, $p^{\alpha} = \nu_i(\mathbb{Z}, p)$. Thus, $p^r - p^{u_1} + b_{u_1}$ minimizes.

Let $u_1 = 0$ (thus $p^r - p \leq i < p^r - 1$). Consider $i+1$. Since $i \neq p^t - 1$,

$$w_p((i+1)!) = w_p(i!)$$

$$w_p((i+1-i)(i+1-(i-1))\cdots(i+1-1)(i+1-0)) = \\ w_p((i-(i-1))(i-(i-2))\cdots(i-1)(i-0))$$

$$w_p(i+1-i)w_p((i+1-(i-1))(i+1-(i-2))\cdots(i+1-1)(i+1-0)) = \\ w_p((i-(i-1))(i-(i-2))\cdots(i-1)(i-0))$$

$$w_p((i+1-(i-1))(i+1-(i-2))\cdots(i+1-1)(i+1-0)) = \\ w_p((i-(i-1))(i-(i-2))\cdots(i-1)(i-0)).$$

And since i minimizes, so does $i+1$. P(i) has now been established.

P(j-1) → P(j) $(i \leq j-1 < p^t - 2)$: j is one of the following types:

(a) $i < j < p^r - p^{u_1} + b_{u_1}$

(b) $j = p^r - p^{u_k} + b_{u_k}$

(c) $p^r - p^{u_k} + b_{u_k} < j < p^r - p^{u_{k+1}} + b_{u_{k+1}}$

(d) $p^t - p + b_1 \leq j < p^t - 1$.

If j is of type (a), then we are are attempting to minimize

$$w_p((a_j - (j-1))(a_j - (j-2)) \cdots (a_j - (i+1))(a_j - (p^r - p^{u_1} + b_{u_1}))(a_j - (i-1)) \\ \cdots (a_j - 1)(a_j - 0)).$$

Now consider $a_j = j$. Since $i \equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^r)$, $j \not\equiv i (\text{mod } p^{r+1})$, and $j \not\equiv p^r - p^{u_1} + b_{u_1} (\text{mod } p^{r+1})$, $w_p(j-i) = w_p(j - (p^r - p^{u_1} + b_{u_1}))$. So

$$\begin{aligned} &w_p((j-(j-1))(j-(j-2)) \cdots \\ &\qquad (j-(i+1))(j-(p^r - p^{u_1} + b_{u_1}))(j-(i-1)) \cdots (j-1)(j-0)) \\ &\quad = w_p((j-(j-1))(j-(j-2)) \cdots (j-(i+1))(j-i)(j-(i-1)) \cdots \\ &\qquad\qquad (j-1)(j-0)) = w_p(j!). \end{aligned}$$

Thus j minimizes.

If j is of type (b), then we are are attempting to minimize

$$w_p((a_j - (j-1)) \cdots (a_j - (p^r - p^{u_k} + b_{u_k})) \cdots (a_j - (i+1)) \\ \cdot (a_j - (p^t - p^{u_1} + b_{u_1}))(a_j - (i-1)) \cdots (a_j - 1)(a_j - 0)).$$

Consider $a_j = p^r - p^{u_{k+1}} + b_{u_{k+1}}$, where $p^{u_{k+1}}$ is the greatest power of p less than $p^r - (p^r - p^{u_k} + b_{u_k})$. Here

$$w_p((p^r - p^{u_{k+1}} + b_{u_{k+1}} - (j-1)) \cdots (p^r - p^{u_{k+1}} + b_{u_{k+1}} - (p^r - p^{u_k} + b_{u_k})) \\ \cdots (p^r - p^{u_{k+1}} + b_{u_{k+1}} - 1)(a_j - 0)) = p^{\beta},$$

where

$$\begin{aligned} \beta = &\left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p) | 0 \leq n \leq p^r - p^{u_k} + b_{u_k}, n \neq i\}\right| + \\ &\left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^2) \mid 0 \leq n \leq p^r - p^{u_k} + b_{u_k}, n \neq i\}\right| + \\ &\cdots + \left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^{r-1}) \mid 0 \leq n \leq p^r - p^{u_k} + b_{u_k}, n \neq i\}\right|. \end{aligned}$$

First, since $i \equiv p^r - p^{u_k} + b_{u_k} (\text{mod } p^{u_k})$ and $i \not\equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^{u_k})$,

$$\left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^v) \mid 0 \leq n \leq p^r - p^{u_k} + b_{u_k}, n \neq i\}\right| = \\ \left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^v) \mid 0 \leq n < p^r - p^{u_k} + b_{u_k}\}\right|,$$

$\forall v \geq 1$.

So for p^v where $u_{k+1} < v < r$, $p^r - p^v \leq p^r - p^{u_k} + b_{u_k}, p^r - p^{u_{k+1}} + b_{u_{k+1}} < p^r$; thus $\lfloor \frac{p^r - p^{u_{k+1}} + b_{u_{k+1}}}{p^v} \rfloor = \lfloor \frac{p^r - p^{u_k} + b_{u_k}}{p^v} \rfloor$. Now

$$\left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^v) \mid 0 \leq n < p^r - p^{u_k} + b_{u_k}\}\right| \leq \lfloor \frac{p^r - p^{u_{k+1}} + b_{u_{k+1}}}{p^v} \rfloor,$$

so $\left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^v) \mid 0 \leq n < p^r - p^{u_k} + b_{u_k}\}\right| \leq \lfloor \frac{p^r - p^{u_k} + b_{u_k}}{p^v} \rfloor$. For p^y where $1 \leq y \leq u_1$, $p^r - p^{u_k} + b_{u_k} \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^y)$. Thus

$$\begin{aligned} &\left|\{n \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^y) \mid 0 \leq n < p^r - p^{u_k} + b_{u_k}\}\right| = \\ &\qquad |\{n \equiv p^r - p^{u_k} + b_{u_k} (\text{mod } p^y) \mid 0 \leq n < p^r - p^{u_k} + b_{u_k}\}| = \\ &\qquad\qquad \lfloor \frac{p^r - p^{u_k} + b_{u_k}}{p^v} \rfloor. \end{aligned}$$

Together we have that

$$p^\beta \leq p^{\lfloor \frac{p^r - p^{u_k} + b_{u_k}}{p} \rfloor + \lfloor \frac{p^r - p^{u_k} + b_{u_k}}{p^2} \rfloor + \cdots + \lfloor \frac{p^r - p^{u_k} + b_{u_k}}{p^{r-1}} \rfloor} = \nu_{p^r - p^{u_k} + b_{u_k}}(\mathbb{Z}, p).$$

And since $\nu_{p^r - p^{u_k} + b_{u_k}}(\mathbb{Z}, p) | p^\beta$, $p^\beta = \nu_{p^r - p^{u_k} + b_{u_k}}(\mathbb{Z}, p)$. Thus, $p^r - p^{u_{k+1}} + b_{u_{k+1}}$ minimizes.

If j is of type (c), then we are are attempting to minimize

$$\begin{aligned} &w_p((a_j - (j-1))(a_j - (j-2)) \cdots (a_j - (p^r - p^{u_{k+1}} + b_{u_{k+1}})) \cdots \\ &\qquad (a_j - (i+1))(a_j - (i-1)) \cdots (a_j - 1)(a_j - 0)). \end{aligned}$$

Now consider $a_j = j$. Since $i \equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^{u_{k+1}+1})$, $j \not\equiv i (\text{mod } p^{u_{k+1}+1})$, and $j \not\equiv p^r - p^{u_{k+1}} + b_{u_{k+1}} (\text{mod } p^{u_{k+1}+1})$, $w_p(j - i) = w_p(j - (p^r - p^{u_{k+1}} + b_{u_{k+1}}))$. So

$$\begin{aligned} &w_p((j - (j-1))(j - (j-2)) \cdots (j - (p^r - p^{u_{k+1}} + b_{u_{k+1}})) \\ &\qquad \cdots (j - (i+1))(j - (i-1)) \cdots (j-1)(j-0)) = \\ &w_p((j - (j-1))(j - (j-2)) \cdots (j - (i+1))(j - i)(j - (i-1)) \cdots (j-1)(j-0)) \\ &\qquad = w_p(j!). \end{aligned}$$

Thus j minimizes.

Let j be of type (d). We need to minimize

$$w_p((a_j + 1 - j)(a_j + 1 - (j-1)) \cdots (a_j - (i+1))(a_j - (i-1)) \cdots (a_j + 1 - 1)(a_j + 1 - 0)).$$

Consider $j+1$. Since $j \neq p^t - 1$,

$$w_p((j+1)!) = w_p(j!)$$

$$w_p((j+1-j)(j+1-(j-1))\cdots(j+1-i)\cdots(j+1-1)(j+1-0)) =$$
$$w_p((j-(j-1))(j-(j-2))\cdots(j-1)(j-0))$$

$$w_p(j+1-i)w_p((j+1-j)(j+1-(j-1))\cdots(j+1-1)(j+1-0)) =$$
$$w_p((j-(j-1))(j-(j-2))\cdots(j-1)(j-0))$$

$$w_p((j+1-j)(j+1-(j-1))\cdots(j+1-1)(j+1-0)) = w_p(j!).$$

And since $w_p(j!)$ is minimal, $j+1$ minimizes.

Thus P(j-1) → P(j) ($i \leq j-1 < p^t - 2$) has been established. Therefore the p-ordering is valid.

The following is a MAPLE program which determines the factorial sequence for a finite $S \subseteq \mathbb{Z}$. genfactall(S) generates this factorial sequence, whereas pordering(p,S) generates a p-ordering for a given p. All other functions below are subsidiary.

```
> with(numtheory):

> orderprod:=proc(A,r)
>    local n,i,prod;
>    n:=nops(A):
>    prod:=1:
>    for i from 1 to n do
>       prod:=prod*(r-A[i]):
>    od:
>    RETURN(prod):
>    end:


> pfactorset:=proc(S)
>    local n,i,j,T;
>    T:={}:
>    n:=nops(S):
>    for i from 1 to n do
>       for j from 1 to n do
>       if i=j then
>       T:=T:
>       elif S[i]-S[j]=-1 then
>       T:=T:
>       else
>       T:=T union factorset(S[i]-S[j]):
>       fi:
>       od:
>    od:
>    RETURN(T):
>    end:


> powerp:=proc(p,x)
>    local pow,y;
>    pow:=0:
>    y:=x:
>    while member(p,factorset(y)) do
>    pow:=pow+1;
>       y:=y/p;
>    od:
```

```
>    RETURN(p∧pow):
>    end:

> nextpick:=proc(p,A,R)
>    local a,n,b,i;
>    n:=nops(R):
>    a:=R[1]:
>    b:=powerp(p,orderprod(A,R[1])):
>    for i from 1 to n do
>       if powerp(p,orderprod(A,R[i]))¡b then
>       b:=powerp(p,orderprod(A,R[i])):
>       a:=R[i]:
>       else
>       b:=b:
>       a:=a:
>       fi:
>    od:
>    RETURN(a):
>    end:

> func:=proc(p,A,R,k)
>    local ans,b,B,S,i;
>    B:=A:
>    S:=R:
>    for i from 1 to k-1 do
>       b:=nextpick(p,B,S):
>       B:=B union {b}:
>       S:=S minus {b}:
>    od:
>    ans:=powerp(p,orderprod(B,nextpick(p,B,S))):
>    RETURN(ans):
>    end:

> genfact:=proc(S,k)
>    local T,A,R,n,m,i,kS;
>    n:=nops(S):
>    kS:=1:
>    if k>=n then
>    kS:=0:
>    else
>       T:=pfactorset(S):
```

```
>       m:=nops(T):
>       A:={S[1]}:
>       R:=S minus {S[1]}:
>       for i from 1 to m do
>       kS:=kS*func(T[i],A,R,k):
>       od:
>    fi:
>    RETURN(kS):
>    end:


> pordering:=proc(p,S)
>    local A,R,O,n,b,i;
>    A:={S[1]}:
>    R:=S minus {S[1]}:
>    n:=nops(R):
>    O:=[S[1]]:
>    while n>0 do
>       b:=nextpick(p,A,R);
>       R:=R minus b;
>       A:=A union b;
>       n:=nops(R);
>       O:=[op(O),b];
>    od:
>    RETURN(O):
>    end:


> genfactall:=proc(S)
>    local n,A,k;
>    n:=nops(S):
>    A:=[genfact(S,1)]:
>    for k from 2 to n-1 do
>       A:=[op(A),genfact(S,k)]:
>    od:
>    RETURN(A):
>    end:
```